

IN THE U.S. PATENT AND TRADEMARK OFFICE

CLAIM TO PRIORITY

December 8, 2003

Applicant(s) herewith claim(s) the benefit of the priority filing date of the following application(s) for the above-entitled U.S. application under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55:

Attachment(s): 1 Certified Copy(ies)

US

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 2 月 9 日
Date of Application:

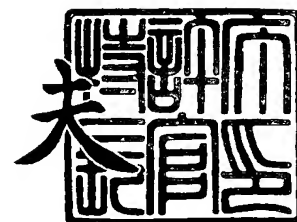
出 願 番 号 特 願 2 0 0 2 - 3 5 6 8 3 9
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 5 6 8 3 9]

出 願 人 日 本 電 気 株 式 会 社
Applicant(s):

2 0 0 3 年 1 0 月 2 9 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



【書類名】 特許願

【整理番号】 41810247

【提出日】 平成14年12月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 11/30

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

 【氏名】 益弘 麻央

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

 【氏名】 渡辺 康弘

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100088959

 【弁理士】

 【氏名又は名称】 境 廣巳

【手数料の表示】

 【予納台帳番号】 009715

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9002136

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 クライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法および装置

【特許請求の範囲】

【請求項 1】 複数のクライアント装置とサーバ装置とがネットワークを通じて接続されたクライアント・サーバ型分散システムにおいて、前記サーバ装置は、サーバ側コンソールから、利用者認証情報と前記クライアント装置の指定を含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付ける要求受付手段と、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段とを備え、前記それぞれのクライアント装置は、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段と、前記サーバ装置から前記ネットワークを通じて前記利用者認証情報設定要求を受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、前記サーバ装置から前記ネットワークを通じて前記利用者認証情報設定無効要求を受信したときに前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段とを備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 2】 請求項 1 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記それぞれのクライアント装置における前記利用者認証手段への利用者認証情報の設定は、前記サーバ側コンソールからのみ設定可能としたことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 3】 請求項 1 または 2 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記サーバ装置は、前記要求転送手段が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段を備え、前記それぞれのクライアント装置に、前記リモート要求処理手段が受信した利用者認証情報設定要求中の暗号化された利用者認証情報を

復号化する復号化手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 4】 請求項 1 または 2 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記それぞれのクライアント装置は、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 5】 請求項 1 または 2 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 6】 請求項 5 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 7】 請求項 6 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間延長手段は、前記保守インタフェースを開放してから初回のログイン要求があった際に、前記利用時間管理手段で管理されている残り利用時間が予め定められた一定時間以内かどうかを判定し、一定時間以内であれば予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長するものであることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 8】 請求項 6 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間延長手段は、前記保守インタフェースを開放してからの初回のログイン中、前記利用時間管理手段で管理されている残り利用時間が予め定められた一定時間以内となったかどうかを判定し、一定時間以内になった場合に予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長するものであることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 9】 請求項 5 または 6 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間管理手段は、前記利用可能時間として前記サーバ装置から送信された前記利用者認証情報設定要求で指定された利用可能時間を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 10】 請求項 5 または 6 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間管理手段は、前記利用可能時間として前記クライアント装置に予め記憶されている利用可能時間基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 11】 請求項 5 または 6 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間管理手段は、前記利用可能時間として、前記サーバ装置から送信された前記利用者認証情報設定要求で利用可能時間が指定されているときは該指定された利用可能時間を使用し、指定されていないときは前記クライアント装置に予め記憶されている利用可能時間基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 12】 請求項 1 または 2 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している

利用者の利用を強制的に不可能にするログイン回数管理手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 13】 請求項 12 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記ログイン回数管理手段は、前記ログイン可能回数として前記サーバ装置から送信された前記利用者認証情報設定要求で指定されたログイン可能回数を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 14】 請求項 13 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記ログイン回数管理手段は、前記ログイン可能回数として前記クライアント装置に予め記憶されているログイン可能回数基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 15】 請求項 13 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記ログイン回数管理手段は、前記ログイン可能回数として、前記サーバ装置から送信された前記利用者認証情報設定要求でログイン可能回数が指定されているときは該指定されたログイン可能回数を使用し、指定されていないときは前記クライアント装置に予め記憶されているログイン可能回数基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 16】 請求項 1 または 2 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段を備えることを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置。

【請求項 17】 a) サーバ装置が、サーバ側コンソールから、利用者認証情報とクライアント装置の指定とを含む利用者認証情報設定要求を受け付け、指定された前記クライアント装置にネットワークを通じて転送するステップと、

b) 前記クライアント装置が、前記ネットワークを通じて前記利用者認証情報設定要求を受信し、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定するステップと、

c) 前記サーバ装置が、前記サーバ側コンソールから、前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付け、指定された前記クライアント装置に前記ネットワークを通じて転送するステップと、

d) 前記クライアント装置が、前記ネットワークを通じて前記利用者認証情報設定無効要求を受信し、前記利用者認証手段に設定されている利用者認証情報を無効にするステップと、

を含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 18】 請求項 17 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記それぞれのクライアント装置における前記利用者認証手段への利用者認証情報の設定は、前記サーバ側コンソールからのみ設定可能としたことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 19】 請求項 17 または 18 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップ a は、前記サーバ装置が前記転送する利用者認証情報を暗号化する処理を含み、前記ステップ b は、前記クライアント装置が前記受信した利用者認証情報を復号化する処理を含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 20】 請求項 17 または 18 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップ b は、前記利用者認証手段に既に設定されている利用者認証情報が前記受信した新たな利用者認証情報に再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする処理を含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 21】 請求項 17 または 18 記載のクライアント・サーバ型分散

システムにおける保守インタフェース利用者認証方法において、

e) それぞれの前記クライアント装置が、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするステップを含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 22】 請求項 21 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、

f) それぞれの前記クライアント装置が、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用可能時間を延長するステップを含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 23】 請求項 22 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップ f は、前記保守インタフェースを開放してから初回のログイン要求があった際に、前記ステップ e で管理されている残り利用時間が予め定められた一定時間以内かどうかを判定し、一定時間以内であれば予め定められた延長時間だけ前記残り利用時間を延長することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 24】 請求項 22 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップ f は、前記保守インタフェースを開放してからの初回のログイン中、前記ステップ e で管理されている残り利用時間が予め定められた一定時間以内となったかどうかを判定し、一定時間以内になった場合に予め定められた延長時間だけ前記残り利用時間を延長することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 25】 請求項 21 または 22 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップ e

における前記利用可能時間として前記サーバ装置から送信された前記利用者認証情報設定要求で指定された利用可能時間を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 26】 請求項 21 または 22 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップ e における前記利用可能時間として前記クライアント装置に予め記憶されている利用可能時間基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 27】 請求項 21 または 22 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップ e における前記利用可能時間として、前記サーバ装置から送信された前記利用者認証情報設定要求で利用可能時間が指定されているときは該指定された利用可能時間を使用し、指定されていないときは前記クライアント装置に予め記憶されている利用可能時間基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 28】 請求項 17 または 18 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、
e) それぞれの前記クライアント装置が、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするステップを含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 29】 請求項 28 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップ e における前記ログイン可能回数として前記サーバ装置から送信された前記利用者認証情報設定要求で指定されたログイン可能回数を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 30】 請求項 29 記載のクライアント・サーバ型分散システムに

における保守インタフェース利用者認証方法において、前記ステップ e における前記ログイン可能回数として前記クライアント装置に予め記憶されているログイン可能回数基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 3 1】 請求項 2 9 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップ e における前記ログイン可能回数として、前記サーバ装置から送信された前記利用者認証情報設定要求でログイン可能回数が指定されているときは該指定されたログイン可能回数を使用し、指定されていないときは前記クライアント装置に予め記憶されているログイン可能回数基準値を使用することを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 3 2】 請求項 1 7 または 1 8 記載のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、
e) それぞれの前記クライアント装置が、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にするステップを含むことを特徴とするクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法。

【請求項 3 3】 複数のクライアント装置とネットワークを通じて接続されるサーバ装置において、サーバ側コンソールから、前記クライアント装置が保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定する利用者認証情報と前記クライアント装置の指定とを含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付ける要求受付手段と、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段とを備えることを特徴とするサーバ装置。

【請求項 3 4】 請求項 3 3 記載のサーバ装置において、前記要求転送部が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段を備えることを特徴とするサーバ装置。

【請求項 3 5】 請求項 3 3 記載のサーバ装置において、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段に設定する前記利用可能時間を、前記利用者認証情報設定要求に含めて送信する構成を備えることを特徴とするサーバ装置。

【請求項 3 6】 請求項 3 3 記載のサーバ装置において、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段に設定する前記ログイン可能回数を、前記利用者認証情報設定要求に含めて送信する構成を備えることを特徴とするサーバ装置。

【請求項 3 7】 サーバ装置にネットワークを通じて接続されるクライアント装置において、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段と、利用者認証情報を含む利用者認証情報設定要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、利用者認証情報設定無効要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段を備えることを特徴とするクライアント装置。

【請求項 3 8】 請求項 3 7 記載のクライアント装置において、前記利用者認証手段への利用者認証情報の設定は、前記サーバ装置から受信した利用者認証情報設定要求のみにより可能としたことを特徴とするクライアント装置。

【請求項 3 9】 請求項 3 7 または 3 8 記載のクライアント装置において、前記サーバ装置から前記ネットワークを通じて受信した前記利用者認証情報設定要求中の暗号化された利用者認証情報を復号化する復号化手段を備えることを特徴とするクライアント装置。

【請求項 4 0】 請求項 3 7 または 3 8 記載のクライアント装置において、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段を備えることを特徴とするクライアント装置。

【請求項 4 1】 請求項 3 7 または 3 8 記載のクライアント装置において、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段を備えることを特徴とするクライアント装置。

【請求項 4 2】 請求項 4 1 記載のクライアント装置において、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段を備えることを特徴とするクライアント装置。

【請求項 4 3】 請求項 3 7 または 3 8 記載のクライアント装置において、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段を備えることを特徴とするクライアント装置。

【請求項 4 4】 請求項 3 7 または 3 8 記載のクライアント装置において、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段を備えることを特徴とするクライアント装置。

【請求項 4 5】 複数のクライアント装置とネットワークを通じて接続されるサーバ装置を構成するコンピュータを、サーバ側コンソールから、前記クライアント装置が保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定する利用者認証情報と前記クライアント装置の指定とを含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定

無効要求を受け付ける要求受付手段、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段、として機能させることを特徴とするサーバプログラム。

【請求項 4 6】 請求項 4 5 記載のサーバプログラムにおいて、前記コンピュータを、更に、前記要求転送手段が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段として機能させるサーバプログラム。

【請求項 4 7】 請求項 4 5 記載のサーバプログラムにおいて、前記要求受付手段および前記要求転送手段は、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段に設定する前記利用可能時間を、前記サーバ側コンソールから受け付けて前記利用者認証情報設定要求に含めて転送することを特徴とするサーバプログラム。

【請求項 4 8】 請求項 4 5 記載のサーバプログラムにおいて、前記要求受付手段および前記要求転送手段は、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段に設定する前記ログイン可能回数を、前記サーバ側コンソールから受け付けて前記利用者認証情報設定要求に含めて転送することを特徴とするサーバプログラム。

【請求項 4 9】 サーバ装置にネットワークを通じて接続されるクライアント装置を構成するコンピュータを、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段、利用者認証情報を含む利用者認証情報設定要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、利用者認証情報設定無効要求を前記ネットワークを通じて前記サーバ装置から受信したとき

に前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段、として機能させることを特徴とするクライアントプログラム。

【請求項 5 0】 請求項 4 9 記載のクライアントプログラムにおいて、前記利用者認証手段への利用者認証情報の設定は、前記サーバ装置から受信した利用者認証情報設定要求のみにより可能としたことを特徴とするクライアントプログラム。

【請求項 5 1】 請求項 4 9 または 5 0 記載のクライアントプログラムにおいて、前記コンピュータを、更に、前記サーバ装置から前記ネットワークを通じて受信した前記利用者認証情報設定要求中の暗号化された利用者認証情報を復号化する復号化手段として機能させることを特徴とするクライアントプログラム。

【請求項 5 2】 請求項 4 9 または 5 0 記載のクライアントプログラムにおいて、前記コンピュータを更に、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段として機能させることを特徴とするクライアントプログラム。

【請求項 5 3】 請求項 4 9 または 5 0 記載のクライアントプログラムにおいて、前記コンピュータを更に、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段として機能させることを特徴とするクライアントプログラム。

【請求項 5 4】 請求項 5 3 記載のクライアントプログラムにおいて、前記コンピュータを更に、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段として機能させることを特徴とするクライアントプログラム。

【請求項 5 5】 請求項 4 9 または 5 0 記載のクライアントプログラムにおいて、前記コンピュータを更に、前記利用者認証手段に利用者認証情報が設定さ

れてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段として機能させることを特徴とするクライアントプログラム。

【請求項 56】 請求項 49 または 50 記載のクライアントプログラムにおいて、前記コンピュータを更に、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段として機能させることを特徴とするクライアントプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はクライアント・サーバ型分散システムにおけるクライアント装置の保守インタフェース利用者認証方法及び装置に関し、特にクライアント装置に設けられた保守インタフェースの利用に際して利用者の認証を行うための利用者認証情報を、ネットワークを通じてサーバ装置から設定でき、また無効化できる保守インタフェース利用者認証方法及び装置に関する。

【0002】

【従来の技術】

クライアント・サーバ型分散システムにおいては、各クライアント装置が地理的に分散して設置されているため、運用時には LAN を介して LAN 上の遠隔保守コンソールから各クライアント装置の遠隔保守を行うことがある。しかしながら、LAN 上からの遠隔保守であるためセキュリティの確保が必要であり、この対策としてクライアント装置の保守インタフェースを予め設定された利用者認証情報を知るものだけが利用できるようにしている。具体的には、クライアント装置に接続されたローカル保守コンソールを用いて、クライアント装置にユーザ名およびパスワードで構成される利用者認証情報を事前に設定しておき、遠隔保守コンソールからログイン、ログアウトと呼ばれる一般的な操作が行われる際に認証用のユーザ名およびパスワードを入力させ、クライアント装置側で登録されてい

るユーザ名およびパスワードとの一致が確認された場合に限り、遠隔保守コンソールからの保守作業を可能としている。

【0 0 0 3】

このように、或る装置の保守を遠隔保守コンソールからネットワークを介して実施する場合に、ユーザ名とパスワードを用いた利用者認証を行うようにした技術は後述する特許文献 1 に記載されている。但し、特許文献 1 には、ユーザ名およびパスワードを事前に登録する具体的な方法は開示されていない。また、後述する特許文献 2 には、インターネットに端末型ダイヤルアップ接続された複数の端末と単一の保守サーバとの間で、OS I 参照モデルのネットワーク層において VPN セッションを実現する IPsec の認証鍵を共有するための端末－保守サーバ間認証鍵共有方法が記載されているが、設定した認証鍵を無効にして保守インタフェースを閉塞する点については記載されていない。

【0 0 0 4】

【特許文献 1】

特許第 3 2 1 4 4 2 3 号

【特許文献 2】

特開 2 0 0 1 - 1 9 7 0 5 8 号公報

【0 0 0 5】

【発明が解決しようとする課題】

ネットワーク上からの遠隔保守のセキュリティを確保するために、上述したようにクライアント装置の保守インタフェースを利用する際には認証情報による利用者認証を実施しているが、事前に設定したユーザ名およびパスワードが漏洩すると、ネットワーク上に接続する他の端末から同様な手順でユーザ名・パスワードが入力されればクライアント装置へアクセス可能となり、保守インタフェースを介してハッキング等の被害にあう可能性がある。システムの運用中にこのようなハッキング等の被害を受ける危険性が生じた場合、クライアント装置に登録されたユーザ名・パスワードを消去したり、別のユーザ名およびパスワードに書き換えることで防御する必要があるが、地理的に分散した各々のクライアント装置の設置場所に出向いてそのローカル保守コンソールから認証情報の消去や変更を行

うのは、手間と時間がかかる上、クライアント側のローカル保守コンソールが既に取り払われていた場合には再接続する手間もかかってしまうという課題がある。また、認証情報を一旦削除してしまうと、運用中における遠隔保守コンソールからの保守ができないため、保守を行う際にはクライアント装置の設置場所に再び出向いて認証情報を設定しなければならない煩わしさもある。つまり、従来のクライアント・サーバ型システムの保守インタフェース利用者認証方式では、セキュリティの確保と保守の容易性を両立するのが困難であった。

【0006】

そこで、本発明の目的は、クライアント装置における保守インタフェースのセキュリティを確保でき、サーバ装置側から複数のクライアント装置の保守インタフェース利用許可／禁止を管理可能なクライアント・サーバ型システムの保守インタフェース利用者認証方法および装置を提供することにある。

【0007】

また、本発明の他の目的は、クライアント装置の保守インタフェースの利用可能時間を管理することで、長時間にわたりクライアント装置の保守インタフェースが開放され続けることによるハッキング等の機会を最小化することが可能なクライアント・サーバ型システムの保守インタフェース利用者認証方法および装置を提供することにある。

【0008】

さらに、本発明の別の目的は、クライアント装置の保守インタフェースの利用可能時間の延長や保守者からの保守インタフェースの閉塞を可能にすることにより、保守インタフェースの利便性を高めたクライアント・サーバ型システムの保守インタフェース利用者認証方法および装置を提供することにある。

【0009】

【課題を解決するための手段】

本発明の第1のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、複数のクライアント装置とサーバ装置とがネットワークを通じて接続されたクライアント・サーバ型分散システムにおいて、前記サーバ装置は、サーバ側コンソールから、利用者認証情報と前記クライアント装置の指定

とを含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付ける要求受付手段と、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段とを備え、前記それぞれのクライアント装置は、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段と、前記サーバ装置から前記ネットワークを通じて前記利用者認証情報設定要求を受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、前記サーバ装置から前記ネットワークを通じて前記利用者認証情報設定無効要求を受信したときに前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段とを備える。

【0010】

この第1のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置にあっては、複数のクライアント装置の保守インタフェースに対するセキュリティ確保のための利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で設定でき、また既に設定されている利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で無効化することができ、個々のクライアント装置の保守インタフェースに対するセキュリティ管理をサーバ側で一括管理することができる。

【0011】

本発明の第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第1のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記それぞれのクライアント装置における前記利用者認証手段への利用者認証情報の設定は、前記サーバ側コンソールからのみ設定可能とする。これにより、個々のクライアント装置の保守インタフェースがサーバ側コンソールからのみ開放でき、より一層セキュリティを確保することができる。

【0012】

本発明の第3のクライアント・サーバ型分散システムにおける保守インタフェー

ス利用者認証装置は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記サーバ装置は、前記要求転送手段が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段を備え、前記それぞれのクライアント装置に、前記リモート要求処理手段が受信した利用者認証情報設定要求中の暗号化された利用者認証情報を復号化する復号化手段を備える。これにより、クライアント装置の保守インタフェースを開放するための利用者認証情報のネットワークからの漏洩が防止でき、セキュリティを確保することができる。

【0013】

本発明の第4のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記それぞれのクライアント装置は、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段を備える。これにより、クライアント装置の保守インタフェースを通じて悪意のアクセスが行われている場合に、サーバ側コンソールからの遠隔制御によって、そのアクセスを直ちに停止させることができると同時に侵入に使った利用者認証情報を無効化し、且つ正規の保守のために新たな利用者認証情報を再設定することができる。

【0014】

本発明の第5のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段を備える。これにより、それぞれのクライアント装置の保守インタフェースが長時間にわたって開放され続け、悪意のアクセス

の危険性が高くなるのを防止することができる。

【0015】

本発明の第6のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第5のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段を備える。具体的には、前記利用時間延長手段は、前記保守インタフェースを開放してから初回のログイン要求があった際に、前記利用時間管理手段で管理されている残り利用時間が予め定められた一定時間以内かどうかを判定し、一定時間以内であれば予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する。また、前記利用時間延長手段は、前記保守インタフェースを開放してからの初回のログイン中、前記利用時間管理手段で管理されている残り利用時間が予め定められた一定時間以内となったかどうかを判定し、一定時間以内になった場合に予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長するものであっても良い。これにより、クライアント装置の保守インタフェースを開放してから実際に保守者がクライアント装置の保守インタフェースを利用するまでに暫く時間がかかり、残り利用時間が短い時点でログインしても十分な保守作業を行うことができ、しかも初回のログインだけ延長を認めるのでセキュリティを確保することができる。

【0016】

ここで、第5または第6のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記利用時間管理手段は、前記利用可能時間として、前記サーバ装置から送信された前記利用者認証情報設定要求で指定された利用可能時間を使用するようにしても良いし、前記クライアント装置に予め記憶されている利用可能時間基準値を使用するようにしても良い。また、前記サーバ装置から送信された前記利用者認証情報設定要求で利用可能時間が指定されているときは該指定された利用可能時間を使用し、指定されていないときは前記クライアント装置に予め記憶されている利用可能時間基準値を使用するよう

しても良い。

【0017】

本発明の第7のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段を備える。これにより、ログイン、ログアウトを何度も繰り返す悪意の利用者に対するセキュリティを確保することができる。

【0018】

ここで、第7のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、前記ログイン回数管理手段は、前記ログイン可能回数として、前記サーバ装置から送信された前記利用者認証情報設定要求で指定されたログイン可能回数を使用するようにしても良いし、前記クライアント装置に予め記憶されているログイン可能回数基準値を使用するようにしても良い。また、前記サーバ装置から送信された前記利用者認証情報設定要求でログイン可能回数が指定されているときは該指定されたログイン可能回数を使用し、指定されていないときは前記クライアント装置に予め記憶されているログイン可能回数基準値を使用するようにしても良い。

【0019】

本発明の第8のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証装置において、それぞれの前記クライアント装置は、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段を備える。これにより、保守作業の終了と同時に保守インタフェースを閉塞でき、クライアント装置の保守インタフェースのセキュリティを確保

することができる。

【0020】

本発明の第1のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、a) サーバ装置が、サーバ側コンソールから、利用者認証情報とクライアント装置の指定とを含む利用者認証情報設定要求を受け付け、指定された前記クライアント装置にネットワークを通じて転送するステップと、b) 前記クライアント装置が、前記ネットワークを通じて前記利用者認証情報設定要求を受信し、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定するステップと、c) 前記サーバ装置が、前記サーバ側コンソールから、前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付け、指定された前記クライアント装置に前記ネットワークを通じて転送するステップと、d) 前記クライアント装置が、前記ネットワークを通じて前記利用者認証情報設定無効要求を受信し、前記利用者認証手段に設定されている利用者認証情報を無効にするステップとを含んで構成される。

【0021】

この第1のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法にあつては、複数のクライアント装置の保守インタフェースに対するセキュリティ確保のための利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で設定でき、また既に設定されている利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で無効化することができ、個々のクライアント装置の保守インタフェースに対するセキュリティ管理をサーバ側で一括管理することができる。

【0022】

本発明の第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第1のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記それぞれのクライアント装置における前記利用者認証手段への利用者認証情報の設定は、前記サーバ側コンソールからのみ設定可能とされる。これにより、個々のクライアント装置の保守インタフェースがサーバ側コンソールからのみ開放でき、より一層セキュリティを確保

することができる。

【0023】

本発明の第3のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップaは、前記サーバ装置が前記転送する利用者認証情報を暗号化する処理を含み、前記ステップbは、前記クライアント装置が前記受信した利用者認証情報を復号化する処理を含んで構成される。これにより、クライアント装置の保守インタフェースを開放するための利用者認証情報のネットワークからの漏洩が防止でき、セキュリティを確保することができる。

【0024】

本発明の第4のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップbは、前記利用者認証手段に既に設定されている利用者認証情報が前記受信した新たな利用者認証情報に再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする処理を含んで構成される。これにより、クライアント装置の保守インタフェースを通じて悪意のアクセスが行われている場合に、サーバ側コンソールからの遠隔制御によって、そのアクセスを直ちに停止させることができると同時に侵入に使った利用者認識情報を無効化し、且つ正規の保守のために新たな利用者認証情報を再設定することができる。

【0025】

本発明の第5のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、e)それぞれの前記クライアント装置が、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするステップを含んで構成される。これにより、それぞれのクラ

クライアント装置の保守インタフェースが長時間にわたって開放され続け、悪意のアクセスの危険性が高くなるのを防止することができる。

【0026】

本発明の第6のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第5のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、f) それぞれの前記クライアント装置が、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用可能時間を延長するステップを含んで構成される。具体的には、前記保守インタフェースを開放してから初回のログイン要求があった際に、前記ステップeで管理されている残り利用時間が予め定められた一定時間以内かどうかを判定し、一定時間以内であれば予め定められた延長時間だけ前記残り利用時間を延長する。また、前記保守インタフェースを開放してからの初回のログイン中、前記ステップeで管理されている残り利用時間が予め定められた一定時間以内となったかどうかを判定し、一定時間以内になった場合に予め定められた延長時間だけ前記残り利用時間を延長するようにしても良い。これにより、クライアント装置の保守インタフェースを開放してから実際に保守者がクライアント装置の保守インタフェースを利用するまでに暫く時間がかかり、残り利用時間が短い時点でログインしても十分な保守作業を行うことができ、しかも初回のログインだけ延長を認めるのでセキュリティを確保することができる。

【0027】

ここで、第5および第6のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップeにおける前記利用可能時間として、前記サーバ装置から送信された前記利用者認証情報設定要求で指定された利用可能時間を使用するようにしても良いし、前記クライアント装置に予め記憶されている利用可能時間基準値を使用するようにしても良い。また、前記サーバ装置から送信された前記利用者認証情報設定要求で利用可能時間が指定されているときは該指定された利用可能時間を使用し、指定されていないときは前記クライアント装置に予め記憶されている利用可能時間基準値を使用するようにしても良い。

【0028】

本発明の第7のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、e) それぞれの前記クライアント装置が、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするステップを含んで構成される。これにより、ログイン、ログアウトを何度も繰り返す悪意の利用者に対するセキュリティを確保することができる。

【0029】

ここで、第7のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、前記ステップeにおける前記ログイン可能回数として、前記サーバ装置から送信された前記利用者認証情報設定要求で指定されたログイン可能回数を使用するようにしても良いし、前記クライアント装置に予め記憶されているログイン可能回数基準値を使用するようにしても良い。また、前記サーバ装置から送信された前記利用者認証情報設定要求でログイン可能回数が指定されているときは該指定されたログイン可能回数を使用し、指定されていないときは前記クライアント装置に予め記憶されているログイン可能回数基準値を使用するようにしても良い。

【0030】

本発明の第8のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法は、第1または第2のクライアント・サーバ型分散システムにおける保守インタフェース利用者認証方法において、e) それぞれの前記クライアント装置が、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にするステップを含んで構成される。これにより、保守作業の終了と同時に保守インタフェースを閉塞でき、クライアント装置の保守インタフェースのセキュリティを確保することができる。

【0031】

本発明の第1のサーバ装置は、複数のクライアント装置とネットワークを通じて接続されるサーバ装置において、サーバ側コンソールから、前記クライアント装置が保守インタフェースの利用に際して利用者の認証を行う利用者認証手段に設定する利用者認証情報と前記クライアント装置の指定とを含む利用者認証情報設定要求、および前記クライアント装置の指定を含む利用者認証情報設定無効要求を受け付ける要求受付手段と、前記要求受付手段で受け付けられた前記利用者認証情報設定要求および前記利用者認証情報設定無効要求を指定された前記クライアント装置に前記ネットワークを通じて転送する要求転送手段とを備える。

【0032】

この第1のサーバ装置にあつては、複数のクライアント装置の保守インタフェースに対するセキュリティ確保のための利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で設定でき、また既に設定されている利用者認証情報をネットワーク経由でサーバ側コンソールから遠隔で無効化することができ、個々のクライアント装置の保守インタフェースに対するセキュリティ管理をサーバ側で一括管理することができる。

【0033】

本発明の第2のサーバ装置は、第1のサーバ装置において、前記要求転送部が転送する利用者認証情報設定要求中の利用者認証情報を暗号化する暗号化手段を備える。これにより、クライアント装置の保守インタフェースを開放するための利用者認証情報のネットワークからの漏洩が防止でき、セキュリティを確保することができる。

【0034】

本発明の第3のサーバ装置は、第1のサーバ装置において、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段に設定する前記利用可能時間を、前記利用者認証情報設定要求に含めて送信する構成を備える。これにより、それぞれのクラ

クライアント装置の保守インタフェースが長時間にわたって開放され続け悪意のアクセスの危険性が高くなるのを防止するために使用する利用可能時間を、サーバ装置から遠隔でそれぞれのクライアント装置に設定することができる。

【0035】

本発明の第4のサーバ装置は、第1のサーバ装置において、それぞれの前記クライアント装置が前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段に設定する前記ログイン可能回数を、前記利用者認証情報設定要求に含めて送信する構成を備える。これにより、ログイン、ログアウトを何度も繰り返す悪意の利用者に対するセキュリティを確保するためのログイン可能回数を、サーバ装置から遠隔で設定することができる。

【0036】

本発明の第1のクライアント装置は、サーバ装置にネットワークを通じて接続されるクライアント装置において、保守インタフェースの利用に際して利用者の認証を行う利用者認証手段と、利用者認証情報を含む利用者認証情報設定要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証情報設定要求に含まれる利用者認証情報を前記利用者認証手段に設定し、利用者認証情報設定無効要求を前記ネットワークを通じて前記サーバ装置から受信したときに前記利用者認証手段に設定されている利用者認証情報を無効にするリモート要求処理手段を備える。

【0037】

この第1のクライアント装置にあつては、保守インタフェースに対するセキュリティ確保のための利用者認証情報をネットワーク経由でサーバ装置から遠隔で設定でき、また既に設定されている利用者認証情報をネットワーク経由でサーバ装置から遠隔で無効化することができ、クライアント装置の保守インタフェースに対するセキュリティ管理をサーバ側で管理することができる。

【0038】

本発明の第2のクライアント装置は、第1のクライアント装置において、前記利用者認証手段への利用者認証情報の設定は、前記サーバ装置から受信した利用者認証情報設定要求のみにより可能とした構成を有する。これにより、クライアント装置の保守インタフェースがサーバ装置からのみ開放でき、より一層セキュリティを確保することができる。

【0039】

本発明の第3のクライアント装置は、第1または第2のクライアント装置において、前記サーバ装置から前記ネットワークを通じて受信した前記利用者認証情報設定要求中の暗号化された利用者認証情報を復号化する復号化手段を備える。これにより、クライアント装置の保守インタフェースを開放するための利用者認証情報のネットワークからの漏洩が防止でき、セキュリティを確保することができる。

【0040】

本発明の第4のクライアント装置は、第1または第2のクライアント装置において、前記利用者認証手段に既に設定されている利用者認証情報が前記ネットワークを通じて受信した新たな利用者認証情報設定要求によって再設定された場合に、前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする強制切断手段を備える。これにより、クライアント装置の保守インタフェースを通じて悪意のアクセスが行われている場合に、サーバ装置からの遠隔制御によって、そのアクセスを直ちに停止させることができると同時に侵入に使った利用者認証情報を無効化し、且つ正規の保守のために新たな利用者認証情報を再設定することができる。

【0041】

本発明の第5のクライアント装置は、第1または第2のクライアント装置において、前記利用者認証手段に利用者認証情報が設定されてから利用可能時間が経過したときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にする利用時間管理手段を備える。これにより、クライアント装置の保守インタフェースが長時間にわたって開放され続け、悪意のアクセスの危険性が高くな

るのを防止することができる。

【0042】

本発明の第6のクライアント装置は、第5のクライアント装置において、前記保守インタフェースを開放してからの初回のログインに限り、予め定められた延長時間だけ前記利用時間管理手段の残り利用時間を延長する利用時間延長手段を備える。これにより、クライアント装置の保守インタフェースを開放してから実際に保守者がクライアント装置の保守インタフェースを利用するまでに暫く時間がかかり、残り利用時間が短い時点でログインしても十分な保守作業を行うことができ、しかも初回のログインだけ延長を認めるのでセキュリティを確保することができる。

【0043】

本発明の第7のクライアント装置は、第1または第2のクライアント装置において、前記利用者認証手段に利用者認証情報が設定されてからログイン可能回数のログインが行われたときに、前記利用者認証手段に設定されている利用者認証情報を無効にすると共に前記保守インタフェースを現に利用している利用者の利用を強制的に不可能にするログイン回数管理手段を備える。これにより、ログイン、ログアウトを何度も繰り返す悪意の利用者に対するセキュリティを確保することができる。

【0044】

本発明の第8のクライアント装置は、第1または第2のクライアント装置において、前記保守インタフェースの利用者が前記保守インタフェースの利用を終了する際に前記利用者認証手段に設定されている利用者認証情報を無効にする認証無効化手段を備える。これにより、保守作業の終了と同時に保守インタフェースを閉塞でき、クライアント装置の保守インタフェースのセキュリティを確保することができる。

【0045】

【発明の実施の形態】

次に本発明の実施の形態について図面を参照して詳細に説明する。

【0046】

【発明の第1の実施の形態】

図1を参照すると、本発明の第1の実施の形態にかかるクライアント・サーバ型システムは、サーバ装置1と複数のクライアント装置3と遠隔保守コンソール5とがLAN6を通じて相互に通信可能に接続されている。また、サーバ装置1にはシリアルインタフェース等を通じてローカル保守コンソール2が接続されており、クライアント装置3にはシリアルインタフェース等を通じてローカル保守コンソール4が接続されている。以下、サーバ装置1に接続されたローカル保守コンソールをサーバ側ローカル保守コンソールと呼び、クライアント装置3に接続されたローカル保守コンソールをクライアント側ローカル保守コンソールと呼ぶ。クライアント側ローカル保守コンソール4は、クライアント装置3のシステムデータの設定や変更などを行うためにクライアント装置3の工事期間等に臨時に設置されるもので、運用中には接続しておかなくとも良い。これに対してサーバ側ローカル保守コンソール2は、サーバ装置3の障害や処理能力の監視、システムデータの設定や変更などを行うもので、運用中は必要時に接続される。例えば本発明をVoIPシステムであるクライアント・サーバ型IP-PBXに適用する場合、サーバ装置1は、IP-PBXにおいて呼制御を行うMGC(Media Gateway Controller)に相当し、サーバ側ローカル保守コンソール2はMGCに接続されたコンソールに相当する。また、クライアント装置3は、公衆電話網等との接続を行うMG(Media Gateway)や電話機を収容するMC(Media Converter)あるいはIP電話機に相当し、ローカル保守コンソール4はそれらに接続されたコンソールに相当する。なお、本発明はクライアント・サーバ型IP-PBXにのみ適用が限定されないのは勿論のことである。

【0047】

サーバ装置1は、サーバ側ローカル保守コンソール2からクライアント装置3を指定した利用者認証情報設定要求および利用者認証情報設定無効要求を受け付ける要求受付部11と、この要求受付部11で受け付けられた要求をLAN6を通じて指定されたクライアント装置3に転送する要求転送部12とを含んで構成される。

【0048】

図2はサーバ側ローカル保守コンソール2から利用者認証情報設定要求が入力された際のサーバ装置1の処理例を示すフローチャートである。システム管理者等が、利用者認証情報の設定対象となるクライアント装置3の指定情報（例えばクライアント装置を一意に識別するクライアント装置名など）と、設定したい利用者認証情報としてのユーザ名およびパスワードとを含む利用者認証情報設定要求をサーバ側ローカル保守コンソール2から入力すると、この要求を要求受付部11により受信し（S101）、同じく要求受付部11によりユーザ名およびパスワードの桁数などの正常性をチェックする（S102）。桁数などが所定の条件を満足しない場合、要求は拒否される。問題がなければ、受け付けた利用者認証情報設定要求を要求受付部11から要求転送部12へ伝達する（S103）。次に、要求転送部12により、利用者認証情報設定要求中で指定されているクライアント装置3のIPアドレスを、例えばクライアント装置名とIPアドレスの対応表（図示せず）などを参照して確認し（S104）、このIPアドレスを用いて利用者認証情報設定要求中のユーザ名およびパスワードを含む利用者認証情報設定指示をLAN6経由で対象クライアント装置3へ送信する（S105）。そして、対象クライアント装置3から利用者認証情報設定完了通知が返されてくると、この通知を要求転送部12で受信して（S106）、要求受付部11に伝達し（S107）、要求受付部11がサーバ側ローカル保守コンソール2に利用者認証情報設定完了通知を出力する（S108）。

【0049】

図3はサーバ側ローカル保守コンソール2から利用者認証情報設定無効要求が入力された際のサーバ装置1の処理例を示すフローチャートである。システム管理者等が、利用者認証情報の設定を無効にしたいクライアント装置3を指定した利用者認証情報設定無効要求をサーバ側ローカル保守コンソール2から入力すると、この要求を要求受付部11により受信し（S111）、受信した利用者認証情報設定無効要求を要求受付部11から要求転送部12へ伝達する（S112）。次に、要求転送部12により、利用者認証情報設定無効要求中で指定されているクライアント装置3のIPアドレスを確認し（S113）、このIPアドレスを

用いて利用者認証情報設定無効指示を LAN 6 経由で対象クライアント装置 3 へ送信する (S 1 1 4)。そして、対象クライアント装置 3 から利用者認証情報設定無効完了通知が返されてくると、この通知を要求転送部 1 2 で受信して (S 1 1 5)、要求受付部 1 1 に伝達し (S 1 1 6)、要求受付部 1 1 がサーバ側ローカル保守コンソール 2 に利用者認証情報設定無効完了通知を出力する (S 1 1 7)。

【0050】

他方、各々のクライアント装置 3 は、Telnet インタフェースに代表される保守インタフェース 3 0 を有しており、また、保守対象となる保守対象部 3 1 と、保守対象部 3 4 の保守を行う利用者に対して認証情報に基づく利用者認証を行う利用者認証部 3 2 と、LAN 6 を通じてサーバ装置 1 から送られてくる利用者認証情報設定要求および利用者認証情報設定無効要求を受信し、各要求に応じた処理を実行するリモート要求処理部 3 3 と、クライアント側ローカル保守コンソール 4 から入力される利用者認証情報設定要求および利用者認証情報設定無効要求を受信し、各要求に応じた処理を実行するローカル要求処理部 3 4 と、遠隔保守コンソール 5 など LAN 6 上の装置からクライアント装置 3 へのログインおよびログアウトにかかる処理を実行するログイン・ログアウト処理部 3 5 とを含んで構成される。保守対象部 3 1 は、例えば、クライアント装置 3 を構成するハードウェアおよびソフトウェアの動作状況および障害状況ならびに各種のシステム設定データを記録するメモリ、ソフトウェアそのものなどである。また、保守対象部 3 1 の保守とは、前記メモリに記憶された動作状況および障害状況の参照や、システム設定データおよびソフトウェアの変更などの操作である。

【0051】

図 4 はサーバ装置 1 から利用者認証情報設定指示が LAN 6 経由で送信されてきた際のクライアント装置 3 の処理例を示すフローチャートである。LAN 経由で利用者認証情報設定指示が送信されてきたクライアント装置 3 は、この指示をリモート要求処理部 3 3 で受信し (S 1 2 1)、指示中のユーザ名およびパスワードが所定の桁数を満たすかどうかのチェックを行う (S 1 2 2)。所定の条件を満たさない場合、この指示は拒否される。問題がなければ、この指示がリモート

要求処理部 33 から利用者認証部 32 に伝達される (S 123)。利用者認識部 32 は伝達された指示中のユーザ名およびパスワードを内部に記憶する (S 124)。他方、リモート要求処理部 33 は、要求元のサーバ装置 3 に対して LAN 6 経由で利用者認証情報設定完了通知を送信する (S 125)。

【0052】

図 5 はサーバ装置 1 から利用者認証情報設定無効指示が LAN 6 経由で送信されてきた際のクライアント装置 3 の処理例を示すフローチャートである。LAN 経由で利用者認証情報設定無効指示が送信されてきたクライアント装置 3 は、この指示をリモート要求処理部 33 で受信し (S 131)、利用者認証部 32 に伝達する (S 132)。利用者認識部 32 は、内部に登録されているユーザ名およびパスワードを消去するなどして無効化する (S 133)。他方、リモート要求処理部 33 は、要求元のサーバ装置 3 に対して LAN 6 経由で利用者認証情報設定無効完了通知を送信する (S 134)。

【0053】

図 6 はクライアント側ローカル保守コンソール 4 から利用者認証情報設定要求が入力された際のクライアント装置 3 の処理例を示すフローチャートである。保守作業等が、設定したい利用者認証情報としてのユーザ名およびパスワードを含む利用者認証情報設定要求をクライアント側ローカル保守コンソール 4 から入力すると、この要求をローカル要求処理部 34 により受信し (S 141)、同じくローカル要求処理部 34 により、要求中のユーザ名およびパスワードが所定の桁数を満たすかどうかのチェックを行う (S 142)。所定の条件を満たさない場合、この要求は拒否される。問題がなければ、要求中のユーザ名およびパスワードを含む利用者認証情報設定指示がローカル要求処理部 34 から利用者認証部 32 に伝達される (S 143)。利用者認識部 32 は伝達された指示中のユーザ名およびパスワードを内部に記憶する (S 144)。他方、ローカル要求処理部 34 は、利用者認証情報設定完了通知をクライアント側ローカル保守コンソール 4 へ出力する (S 145)。

【0054】

図 7 はクライアント側ローカル保守コンソール 4 から利用者認証情報設定無効要

求が入力された際のクライアント装置 3 の処理例を示すフローチャートである。保守作業等が、設定されている利用者認証情報を無効化する利用者認証情報設定無効要求をクライアント側ローカル保守コンソール 4 から入力すると、この要求をローカル要求処理部 34 により受信し (S 151)、利用者認証部 32 に伝達する (S 152)。利用者認証部 32 は、内部に登録されているユーザ名およびパスワードを消去するなどして無効化する (S 153)。他方、ローカル要求処理部 34 は、利用者認証情報設定無効完了通知をクライアント側ローカル保守コンソール 4 へ出力する (S 154)。

【0055】

図 8 は遠隔保守コンソール 5 からユーザ名およびパスワードの指定を含むログイン要求が LAN 6 経由で送信されてきた際のクライアント装置 3 の処理例を示すフローチャートである。LAN 経由でログイン要求が送信されてきたクライアント装置 3 は、このログイン要求をログイン・ログアウト処理部 35 で受信し (S 161)、ログイン要求中のユーザ名およびパスワードが所定の桁数等を満たすかどうかのチェックを行う (S 162)。所定の条件を満たさない場合、このログイン要求は拒否される。問題がなければ、このログイン要求中のユーザ名およびパスワードを指定した認証指示がログイン・ログアウト処理部 35 から利用者認証部 32 に伝達される (S 163)。利用者認証部 32 は、内部の利用者認証情報が事前に登録されているかどうかを判定し (S 164)、登録されていれば (S 165 で YES)、ログイン・ログアウト処理部 35 から伝達された認証指示中のユーザ名およびパスワードと、内部に登録されているユーザ名およびパスワードとを比較する (S 166)。そして、両者が一致した場合 (S 167 で YES)、認証成功を利用者認証部 32 からログイン・ログアウト処理部 35 へ伝達する (S 168)。ログイン・ログアウト処理部 35 は、遠隔保守コンソール 5 からの保守対象部 31 へのアクセスを許容するためのログイン処理を実行し (S 169)、遠隔保守コンソール 5 へログイン許可を通知する (S 170)。これにより、以降、保守作業等は遠隔保守コンソール 5 から LAN 6 経由でクライアント装置 3 の保守対象部 31 へアクセスすることが可能となる。

【0056】

他方、利用者認証部 3 2 で利用者認証情報が事前に登録されていないと判断されたか（S 1 6 5 で N O）、登録されていたが認証指示中のユーザ名およびパスワードが登録されているユーザ名およびパスワードと一致しないと判断された場合（S 1 6 7 で N O）、認証失敗が利用者認証部 3 2 からログイン・ログアウト処理部 3 5 へ伝達され（S 1 7 1）、ログイン・ログアウト処理部 3 5 は、遠隔リモート保守コンソール 5 に対してログイン不許可を通知する（S 1 7 1）。

【 0 0 5 7 】

図 9 はログイン中の遠隔保守コンソール 5 からログアウト要求が L A N 6 経由で送信されてきた際のクライアント装置 3 の処理例を示すフローチャートである。L A N 6 経由でログアウト要求が送信されてきたクライアント装置 3 は、このログアウト要求をログイン・ログアウト処理部 3 5 で受信し（S 1 8 1）、遠隔保守コンソール 5 から保守対象部 3 1 への以後のアクセスを禁止するためのログアウト処理を実行する（S 1 8 2）。そして、ログイン・ログアウト処理部 3 5 により遠隔保守コンソール 5 へログアウト完了通知を送信する（S 1 8 3）。

【 0 0 5 8 】

次に、本実施の形態の動作を説明する。

【 0 0 5 9 】

図 1 0 は本実施の形態の動作例を示すシーケンスチャートであり、以下の 4 つの場面のシーケンスが示されている。

- （1）サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用者認証情報の設定
- （2）利用者認証情報登録後の遠隔保守コンソール 5 によるクライアント装置 3 へのログイン、ログアウト
- （3）サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用者認証情報の無効化
- （4）利用者認証情報無効化後の遠隔保守コンソール 5 によるクライアント装置 3 へのログイン

【 0 0 6 0 】

以下、上記の 4 つの場面について本実施の形態の動作を説明する。

【0061】

(1) 先ず、図1、図2、図4および図10を参照して、サーバ側ローカル保守コンソール2からクライアント装置3へ利用者認証情報を設定する際の動作を説明する。

【0062】

システム管理者等が、サーバ側ローカル保守コンソール2から、クライアント装置3の保守インタフェース30のセキュリティを開放するためのユーザ名およびパスワードと対象とするクライアント装置3の指定とを含む利用者認証情報設定要求を入力すると(図10のR101)、サーバ装置1でこの要求の受付処理が行われる(R102)。この受付処理では、要求受付部11が利用者認証情報設定要求を受信する処理とユーザ名およびパスワードの正常性をチェックする処理とが行われる(図2のS101、S102)。そして問題がなければ、この要求が要求転送部12に伝達される(図2のS103)。次に要求転送部12により、利用者認証情報設定要求中で指定されたクライアント装置3のIPアドレスが取得され(図2のS104)、LAN6を経由してクライアント装置3のリモート要求処理部33へユーザ名およびパスワードを含む利用者認証情報設定指示が送信される(図10のR103、図2のS105)。

【0063】

クライアント装置3は、サーバ装置1から転送されてきた利用者認証情報設定指示をリモート要求処理部33で受信し(図4のS121)、ユーザ名およびパスワードの正常性を確認して(S122)、問題がなければ利用者認証情報設定指示を利用者認証部32に伝達する(S123)。利用者認証部32は、利用者認証情報設定指示中のユーザ名およびパスワードを記憶する(図10のR104、図2のS124)。一方、リモート要求処理部33は、利用者認証情報設定完了通知をLAN6経由でサーバ装置1の要求転送部12に送る(図10のR105、図2のS125)。要求転送部12は、利用者認証情報設定完了通知を受信すると、要求受付部11を通じてサーバ側ローカル保守コンソール2に出力する(図10のR106、図2のS106～S108)。

【0064】

(2) 次に、図1、図8、図9および図10を参照して、利用者認証情報登録後の遠隔保守コンソール5によるクライアント装置3へのログイン、ログアウト時の動作を説明する。

【0065】

クライアント装置3の利用者認証部32にユーザ名およびパスワードで構成される利用者認証情報が登録された後に、保守作業者が、保守作業の準備の一環として遠隔保守コンソール5からLAN6経由でクライアント装置3に対して、ユーザ名およびパスワードを指定したログイン要求を入力すると(図10のR111)、クライアント装置3で利用者認証にかかる一連の処理が実行される(図10のR112、図8のS161～S172)。具体的には、遠隔保守コンソール5からのログイン要求がログイン・ログアウト処理部35で受信されて正常性のチェックが行われ(S161、S162)、問題がなければログイン要求中のユーザ名およびパスワードを含む認証指示が利用者認証部32に出される(S163)。次に利用者認証部32において、利用者認証情報の登録の有無の判定(S164、S165)、登録がある場合の認証指示中のユーザ名およびパスワードと登録されているユーザ名およびパスワードとの一致の判定(S166、S167)が実施される。図10の利用者認証R112では、利用者認証情報が事前に登録されており且つログイン要求で指定されたユーザ名およびパスワードが登録されているユーザ名およびパスワードと一致し、認証成功した場面を想定している。このため、利用者認証部32はログイン・ログアウト処理部35に認証成功を通知し(S168)、ログイン・ログアウト処理部35はログイン処理を行い(S169)、遠隔保守コンソール5に対してログイン許可を通知する(S170、図10のR113)。これにより、保守作業者は、遠隔保守コンソール5からクライアント装置3の保守対象部31に対してアクセスし、各種の保守作業を開始することができる。

【0066】

保守作業者が保守作業を終えたので、遠隔保守コンソール5からログアウト要求を入力すると(図10のR114)、クライアント装置3のログイン・ログアウト処理部35がこれを受信し(図9のS181)、ログアウト処理を実行する(

S182、図10のR115)。そして、ログイン・ログアウト処理部35は、遠隔保守コンソール5に対してログアウト完了通知を送信する(S183、図10のR116)。これにより、遠隔保守コンソール5からのクライアント装置3の保守対象部31へのアクセスは禁止される。但し、利用者認証部32にユーザ名およびパスワードが記憶され、ログイン要求待ちとなっているため、クライアント装置3の保守インタフェース30は開放されている状況である。つまり、クライアント装置3の保守インタフェース30は閉塞されていない。従って、遠隔保守コンソール5から次のログイン要求が来てユーザ名およびパスワードが一致して認証成功すると、クライアント装置3の保守対象部31へのアクセスが再び可能となる。

【0067】

(3) 次に、サーバ側ローカル保守コンソール2からクライアント装置3に登録された利用者認証情報を無効化する際の動作を、図1、図3、図5および図10を参照して説明する。

【0068】

システム管理者等が、サーバ側ローカル保守コンソール2からクライアント装置3の保守インタフェース30を閉塞してセキュリティを確保するために、対象となるクライアント装置3を指定した利用者認証情報設定無効要求を入力すると(図10のR121)、サーバ装置1で利用者認証情報無効要求受付処理が行われる(R122)。この受付処理では、要求受付部11が利用者認証情報設定無効要求を受信する処理とこの受信した要求を要求転送部12に伝達する処理とが行われる(図3のS111、S112)。次に要求転送部12により、利用者認証情報設定無効要求中で指定されたクライアント装置3のIPアドレスが取得され(図3のS113)、LAN6を経由してクライアント装置3のリモート要求処理部33へ利用者認証情報設定無効指示が送信される(図10のR123、図3のS114)。

【0069】

クライアント装置3は、サーバ装置1から転送されてきた利用者認証情報設定無効指示をリモート要求処理部33で受信し(図5のS131)、利用者認証情報

設定無効指示を利用者認証部 3 2 に伝達する (S 1 3 2)。利用者認証部 3 2 は、登録されているユーザ名およびパスワードから構成される利用者認証情報を無効化する (図 1 0 の R 1 2 4、図 5 の S 1 3 3)。一方、リモート要求処理部 3 3 は、利用者認証情報設定無効完了通知を L A N 6 経由でサーバ装置 1 の要求転送部 1 2 に送る (図 1 0 の R 1 2 5、図 5 の S 1 3 4)。要求転送部 1 2 は、利用者認証情報設定無効完了通知を受信すると、要求受付部 1 1 を通じてサーバ側ローカル保守コンソール 2 に出力する (図 1 0 の R 1 2 6、図 3 の S 1 1 5 ~ S 1 1 7)。

【 0 0 7 0 】

(4) 次に、利用者認証情報無効化後に遠隔保守コンソール 5 からクライアント装置 3 へログイン要求があった場合の動作を、図 1、図 8 および図 1 0 を参照して説明する。

【 0 0 7 1 】

遠隔保守コンソール 5 から L A N 6 経由でクライアント装置 3 に対してログイン要求が入力されると (図 1 0 の R 1 3 1)、クライアント装置 3 で利用者認証にかかる一連の処理が実行される (図 1 0 の R 1 3 2、図 8 の S 1 6 1 ~ S 1 7 2)。しかし、利用者認証部 3 2 には利用者認証情報が登録されていないため、認証失敗となる (図 8 の S 1 6 5 で N O)。このため、ログイン・ログアウト処理部 3 5 は、遠隔保守コンソール 5 に対してログイン不許可を通知する (S 1 7 2、図 1 0 の R 1 3 3)。これにより、遠隔保守コンソール 5 からのクライアント装置 3 の保守対象部 3 1 へのアクセスは禁止される。なお、利用者認証部 3 2 にユーザ名およびパスワードが登録されている場合でも、遠隔保守コンソール 5 からのログイン要求で指定したユーザ名およびパスワードが利用者認証部 3 2 に登録されているユーザ名およびパスワードと一致しないときは同様にログイン・ログアウト処理部 3 5 はログイン許可を与えない動作となる。

【 0 0 7 2 】

図 1 1 は本実施の形態の動作例を示すシーケンスチャートであり、以下の 2 つの場面のシーケンスが示されている。

(1) クライアント側ローカル保守コンソール 4 からクライアント装置 3 への利

利用者認証情報の設定

(2) 利用者認証登録後の遠隔保守コンソール 5 によるクライアント装置 3 へのログイン、ログアウト

(3) クライアント側ローカル保守コンソール 4 からクライアント装置 3 への利用者認証情報の無効化

【0073】

以下、上記の 3 つの場面について本実施の形態の動作を説明する。

【0074】

(1) 先ず、図 1、図 6 および図 11 を参照して、クライアント側ローカル保守コンソール 4 からクライアント装置 3 へ利用者認証情報を設定する際の動作を説明する。

【0075】

システム管理者等が、クライアント側ローカル保守コンソール 4 から、クライアント装置 3 の保守インタフェース 30 のセキュリティを開放するためのユーザ名およびパスワードの指定を含む利用者認証情報設定要求を入力すると（図 11 の R141）、クライアント装置 3 は、この利用者認証情報設定要求をローカル要求処理部 34 で受信し（図 6 の S141）、ユーザ名およびパスワードの正常性を確認して（S142）、問題がなければ利用者認証情報設定指示を利用者認証部 32 に伝達する（S143）。利用者認証部 32 は、利用者認証情報設定指示中のユーザ名およびパスワードを記憶する（図 11 の R142、図 6 の S144）。一方、ローカル要求処理部 34 は、利用者認証情報設定完了通知をクライアント側ローカル保守コンソール 4 に出力する（図 11 の R143、図 6 の S145）。

【0076】

(2) 利用者認証登録後の遠隔保守コンソール 5 によるクライアント装置 3 へのログイン、ログアウト時の動作は既に説明した図 10 のシーケンス R111～R116 と同じであるため、説明は省略する。

【0077】

(3) 次に、クライアント側ローカル保守コンソール 4 からクライアント装置 3

に登録された利用者認証情報を無効化する際の動作を、図 1、図 7 および図 11 を参照して説明する。

【0078】

システム管理者等が、クライアント側ローカル保守コンソール 4 からクライアント装置 3 の保守インタフェース 30 を閉塞してセキュリティを確保するために、利用者認証情報設定無効要求を入力すると（図 11 の R151）、クライアント装置 3 は、この利用者認証情報設定無効指示をローカル要求処理部 34 で受信し（図 7 の S151）、利用者認証情報設定無効指示を利用者認証部 32 に伝達する（S152）。利用者認証部 32 は、登録されているユーザ名およびパスワードから構成される利用者認証情報を無効化する（図 11 の R152、図 7 の S153）。一方、ローカル要求処理部 34 は、利用者認証情報設定無効完了通知をクライアント側ローカル保守コンソール 4 へ出力する（図 11 の R153、図 7 の S154）。

【0079】

以上説明したように、本実施の形態によれば、サーバ側ローカル保守コンソール 2 から遠隔地にある複数のクライアント装置 3 の保守インタフェース 30 を開放することができ、且つ、サーバ側ローカル保守コンソールから遠隔地にある複数のクライアント装置 3 の保守インタフェース 30 を閉塞することができる。また、クライアント装置 3 にローカル保守コンソール 4 が接続されている場合には、各クライアント装置毎に、そのクライアント側ローカル保守コンソール 2 からクライアント装置 3 の保守インタフェース 30 の開放、閉塞を行うこともできる。

【0080】

【発明の第 2 の実施の形態】

図 12 を参照すると、本発明の第 2 の実施の形態にかかるクライアント・サーバ型システムは、図 1 に示した第 1 の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置 3 からローカル要求処理部 34 を削除し、クライアント側ローカル保守コンソール 4 からクライアント装置 3 の利用者認証部 32 への利用者認証情報の設定およびその無効化を行えないようにした点で第 1 の実施の形態と相違し、その他の点は第 1 の実施の形態と同じである。

【0081】

本実施の形態においては、サーバ側ローカル保守コンソール2のみからLAN6を経由してクライアント装置3内に遠隔保守コンソール5からLAN6を介してクライアント装置3の保守インタフェース30を開放するための利用者認証情報（ユーザ名およびパスワード）を設定することができ、またサーバ側ローカル保守コンソール2からクライアント装置3に設定した利用者認証情報を削除し、クライアント装置3の保守インタフェース30を利用禁止にすることができる。

【0082】

このようにサーバ側ローカル保守コンソール2のみに限定して複数のクライアント装置3の保守インタフェース30を開放、閉塞できるようにしたことで、保守インタフェース30のセキュリティの管理をサーバ装置1のシステム管理者が容易に管理することが可能となる。

【0083】**【発明の第3の実施の形態】**

図13を参照すると、本発明の第3の実施の形態にかかるクライアント・サーバ型システムは、図12に示した第2の実施の形態にかかるクライアント・サーバ型システムにおけるサーバ装置13に、ユーザ名およびパスワードを暗号化する暗号化部13を備え、各クライアント装置3に、暗号化されたユーザ名およびパスワードを復号化する復号化部36を備えている点で第2の実施の形態と相違し、その他の点は第2の実施の形態と同じである。

【0084】

図14はサーバ側ローカル保守コンソール2から利用者認証情報設定要求が入力された際のサーバ装置1の処理例を示すフローチャートであり、ステップS301～S303が追加されている点が図3のフローチャートと相違する。システム管理者等が、利用者認証情報の設定対象となるクライアント装置3の指定情報と、設定したい利用者認証情報としてのユーザ名およびパスワードとを含む利用者認証情報設定要求をサーバ側ローカル保守コンソール2から入力すると、要求受付部11がこの要求を受信し（S101）、ユーザ名およびパスワードの桁数などの正常性をチェックし（S102）、問題がなければ受け付けた利用者認証情

報設定要求中のユーザ名およびパスワードを要求受付部 11 から暗号化部 13 へ伝達する (S301)。暗号化部 13 は、共通鍵暗号方法や秘密鍵暗号方法などシステムで予め定められた任意の暗号方法により、ユーザ名およびパスワードを暗号化し (S302)、暗号化されたユーザ名およびパスワードを要求受付部 11 に伝達する (S303)。要求受付部 11 は、暗号化されたユーザ名およびパスワードを含む利用者認証情報設定要求を要求転送部 12 へ伝達する (S103)。以下、図 3 を参照して説明した処理と同様の処理が実行される (S104～S108)。

【0085】

図 15 はサーバ装置 1 から利用者認証情報設定指示が LAN 6 経由で送信されてきた際のクライアント装置 3 の処理例を示すフローチャートであり、ステップ S311～S313 が追加されている点が図 4 のフローチャートと相違する。LAN 経由で利用者認証情報設定指示が送信されてきたクライアント装置 3 は、この指示をリモート要求処理部 33 で受信し (S121)、指示中の暗号化されたユーザ名およびパスワードを復号化部 36 へ伝達する (S311)。復号化部 36 は、暗号化されたユーザ名およびパスワードを復号化し (S312)、リモート要求処理部 33 へ伝達する (S313)。リモート要求処理部 33 は、ユーザ名およびパスワードが所定の桁数を満たすかどうかのチェックを行い (S122)、問題がなければ、この指示を利用者認証部 32 に伝達する (S123)。以下、図 4 を参照して説明した処理と同様の処理が実行される (S124、S125)。

【0086】

次に、本実施の形態の動作を説明する。

【0087】

図 16 は本実施の形態の動作例を示すシーケンスチャートであり、サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用者認証情報の設定場面のシーケンスを示す。以下、図 13～図 16 を参照して、サーバ側ローカル保守コンソール 2 からクライアント装置 3 へ利用者認証情報を設定する際の動作を説明する。

【0088】

システム管理者等が、サーバ側ローカル保守コンソール2から、クライアント装置3の保守インタフェース30のセキュリティを開放するためのユーザ名およびパスワードと対象とするクライアント装置3の指定とを含む利用者認証情報設定要求を入力すると（図16のR301）、サーバ装置1でこの要求の受付処理が行われる（R302）。この受付処理では、要求受付部11が利用者認証情報設定要求を受信する処理とユーザ名およびパスワードの正常性をチェックする処理とが行われる（図14のS101、S102）。そして問題がなければ、暗号化部13でユーザ名およびパスワードを暗号化する処理が実施される（図14のR303、図14のS301～S303）。そして、暗号化されたユーザ名およびパスワードを含む利用者認証情報設定要求が要求受付部11から要求転送部11へ伝達される（S103）。その後、要求転送部12は、利用者認証情報設定要求中で指定されたクライアント装置3のIPアドレスを取得し（S104）、LAN6を経由してクライアント装置3のリモート要求処理部33へユーザ名およびパスワードを含む利用者認証情報設定指示を送信する（図16のR304、図14のS105）。

【0089】

クライアント装置3は、サーバ装置1から転送されてきた利用者認証情報設定指示をリモート要求処理部33で受信し（図15のS121）、指示中に含まれる暗号化されたユーザ名およびパスワードを復号化部36を用いて復号化する（図16のR305、図15のS311～S313）。続いて、復号化されたユーザ名およびパスワードの正常性を確認し（S122）、問題がなければ利用者認証情報設定指示を利用者認証部32に伝達する（S123）。利用者認証部32は、利用者認証情報設定指示中のユーザ名およびパスワードを記憶する（図16のR306、図15のS124）。一方、リモート要求処理部33は、利用者認証情報設定完了通知をLAN6経由でサーバ装置1の要求転送部12に送る（図16のR307、図15のS125）。要求転送部12は、利用者認証情報設定完了通知を受信すると、要求受付部11を通じてサーバ側ローカル保守コンソール2に出力する（図16のR308、図14のS106～S108）。

【0090】

保守者が保守コンソール5を使用してログイン・ログアウトする手順及びサーバ側ローカル保守コンソール2から設定済みのユーザ名・パスワードを無効にする手順など、その他の動作は第2の実施の形態と同様である。

【0091】

以上説明したように本実施の形態によれば、サーバ側ローカル保守コンソール2から複数のクライアント装置3の保守インタフェース30を開放する際に、サーバ装置1とクライアント装置3間で転送するユーザ名およびパスワードから構成される利用者認証情報を暗号化することにより、利用者認証情報の漏洩が防止でき、セキュリティを確保することができる。

【0092】

なお、本実施の形態において、第1の実施の形態と同様にそれぞれのクライアント装置3に図1のクライアント側ローカル保守コンソール4を接続し、クライアント装置3内にローカル要求処理部34を設けるようにしても良い。

【0093】**【発明の第4の実施の形態】**

図17を参照すると、本発明の第4の実施の形態にかかるクライアント・サーバ型システムは、図13に示した第3の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置3に、利用者認証部32の利用者認証情報が再設定される際にクライアント装置3の保守インタフェース30を利用するログイン中の装置があれば該装置に対して強制切断通知を送出して強制切断を実施する強制切断部37を備えている点で第3の実施の形態と相違し、その他の点は第3の実施の形態と同じである。

【0094】

図18はサーバ装置1から利用者認証情報設定指示がLAN6経由で送信されてきた際のクライアント装置3の処理例を示すフローチャートであり、ステップS401～S405が追加されている点が図15のフローチャートと相違する。LAN経由で利用者認証情報設定指示が送信されてきたクライアント装置3は、この指示をリモート要求処理部33で受信し（S121）、この指示中の暗号化さ

れたユーザ名およびパスワードを復号化部 36 で復号化し (S 3 1 1 ~ S 3 1 3)、ユーザ名およびパスワードが所定の桁数を満たすかどうかのチェックを行い (S 1 2 2)、問題がなければ、ユーザ名およびパスワードを含む利用者認証情報設定指示をリモート要求処理部 33 から利用者認証部 32 に伝達する (S 1 2 3)。ここまでは第 3 の実施の形態と同じ動作である。続いて、利用者認証部 32 により利用者認証情報が既に登録されているかどうかを判定し (S 4 0 1)、未登録の場合と既登録の場合とで処理を切り分ける。

【0095】

利用者認証情報が利用者認証部 32 に未だ登録されていないときは、速やかに、利用者認証情報設定指示中のユーザ名およびパスワードを利用者認証部 32 に登録し (S 1 2 4)、リモート要求処理部 33 から利用者認証情報設定完了通知をサーバ装置 1 に送信する (S 1 2 5)。

【0096】

他方、利用者認証情報が利用者認証部 32 に既に登録されていた場合、利用者認証部 32 から強制切断部 37 に対し強制切断処理を依頼する (S 4 0 2)。強制切断部 37 は、ログイン・ログアウト処理部 35 に対してクライアント装置 3 の保守インタフェース 30 を利用するためにログインしている遠隔保守コンソール 5 が存在するかどうかを問い合わせ (S 4 0 3)、存在しない場合には処理完了を利用者認証部 32 に通知する (S 4 0 5)。しかし、ログイン中の遠隔保守コンソール 5 が存在する場合は、その遠隔保守コンソール 5 に対して強制切断通知を送出し、強制切断を行う (S 4 0 4)、そして、処理完了を利用者認証部 32 に通知する (S 4 0 5)。その後、利用者認証部 32 は、利用者認証情報設定指示中のユーザ名およびパスワードを利用者認証部 32 に登録し (S 1 2 4)、リモート要求処理部 33 から利用者認証情報設定完了通知をサーバ装置 1 に送信する (S 1 2 5)。

【0097】

次に本実施の形態の動作を説明する。

【0098】

図 19 は本実施の形態の動作例を示すシーケンスチャートであり、サーバ側ロー

カル保守コンソール 2 から LAN 6 を経由してクライアント装置 3 内にクライアント装置 3 の保守インタフェース 30 を開放するためのユーザ名およびパスワードの初期設定を行った後、何者かが遠隔保守コンソール 5 からクライアント装置 3 にログインして保守対象部 34 にアクセスしている状態で、サーバ側ローカル保守コンソール 2 からクライアント装置 3 の保守インタフェース 30 のユーザ名およびパスワードを再設定し、正規の遠隔保守を行う場面のシーケンスを示す。

【0099】

図 19 のシーケンスのうち、サーバ側ローカル保守コンソール 2 からクライアント装置 3 にユーザ名およびパスワードを初期設定するシーケンス R301～R308 は、図 16 を参照して説明した処理と同じである。この場合、設定前の利用者認証部 32 にはユーザ名およびパスワードが存在しないので、図 18 の処理 S402～S405 はスキップされる。

【0100】

クライアント装置 3 の利用者認証部 32 にユーザ名およびパスワードが設定された後、何者かが遠隔保守コンソール 5 から LAN 6 経由でクライアント装置 3 に対してユーザ名およびパスワードを指定したログイン要求を入力すると（図 19 の R401）、図 8 および図 10 を参照して説明した処理と同様の処理がクライアント装置 3 で実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部 32 に登録されているユーザ名およびパスワードと一致すると、ログインが許可され（図 19 の R402、R403）、遠隔保守コンソール 5 からクライアント装置 3 の保守対象部 31 に対するアクセスが可能となる。

【0101】

このように遠隔保守コンソール 5 がログインしている最中に、サーバ側ローカル保守コンソール 2 から利用者認証情報設定要求が入力された場合（図 19 の R411）、以下のような動作が行われる。

【0102】

まず、サーバ装置 1 の要求受付部 11 が利用者認証情報設定要求をサーバ側ローカル保守コンソール 2 から受信し、その正常性をチェックする受付処理を行う（図 19 の R412）。続いて、暗号化部 13 でユーザ名およびパスワードが暗号

化され（図19のR413）、暗号化されたユーザ名およびパスワードを含む利用者認証情報設定指示が、要求転送部12からLAN6を経由してクライアント装置3のリモート要求処理部33へ送信される（図19のR414）。

【0103】

クライアント装置3は、サーバ装置1から転送されてきた利用者認証情報設定指示をリモート要求処理部33で受信し（図18のS121）、指示中に含まれる暗号化されたユーザ名およびパスワードを復号化部36を用いて復号化する（図19のR415、図18のS311～S313）。続いて、復号されたユーザ名およびパスワードの正常性を確認し（S122）、問題がなければ利用者認証情報設定指示を利用者認証部32に伝達する（S123）。

【0104】

利用者認証部32は、利用者認証情報が既に登録されているため（S401でYES）、強制切断部37に対し強制切断処理を依頼する（S402）。強制切断部37は、ログイン・ログアウト処理部35において遠隔保守コンソール5がログイン中であることを確認し（S403でYES）、遠隔保守コンソール5に対して強制切断通知を送出し、強制切断を行う（図19のR416、図18のS404）、これにより、遠隔保守コンソール5からの保守対象部31へのアクセスは不可能になる。その後、強制切断部37は、処理完了を利用者認証部32に通知し（S405）、利用者認証部32は、既に登録されている利用者認証情報を消去する等して無効化した後、利用者認証情報設定指示中のユーザ名およびパスワードを登録する（図19のR417、図18のS124）。そして、リモート要求処理部33から利用者認証情報設定完了通知がサーバ装置1に送信され（図19のR418、図18のS125）、最終的にサーバ側ローカル保守コンソール2へ通知される（図19のR419）。

【0105】

ユーザ名およびパスワードが再設定された後、保守者が再設定された新たなユーザ名およびパスワードを使って遠隔保守コンソール5からクライアント装置3にログインして保守作業を行い、作業終了時点でログアウトを行う場面のシーケンスR111～R116は、図10を参照して説明したシーケンスと同じである。

【0106】

このように本実施の形態によれば、サーバ側ローカル保守コンソール 2 からクライアント装置 3 の保守インタフェース 30 のユーザ名およびパスワードを設定する指示があった場合、クライアント装置 3 は、利用者認証部 32 に既に利用者認証情報が設定されているときは、遠隔保守コンソール 5 がログイン中であれば強制切断通知を送出して強制切断を行うと共に、利用者認証部 32 にユーザ名およびパスワードを再設定する。従って、クライアント装置 3 の保守インタフェース 30 に対して悪意のアクセスが行われているなどの場合に、サーバ側ローカル保守コンソール 2 からクライアント装置 1 の保守インタフェース 30 のユーザ名およびパスワードを再度設定し直すことで、悪意のアクセスを阻止することができ、同時にユーザ名およびパスワードを再設定することができ、十分なセキュリティを確保することができる。

【0107】

なお、本実施の形態において、第 1 の実施の形態と同様にそれぞれのクライアント装置 3 に図 1 のクライアント側ローカル保守コンソール 4 を接続し、クライアント装置 3 内にローカル要求処理部 34 を設けるようにしても良い。また、利用者認証情報を暗号化せずにサーバ装置 1 からクライアント装置 3 へ転送するようにしても良く、その場合には暗号化部 13 および復号化部 36 は省略される。

【0108】**【発明の第 5 の実施の形態】**

図 20 を参照すると、本発明の第 5 の実施の形態にかかるクライアント・サーバ型システムは、図 17 に示した第 4 の実施の形態にかかるクライアント・サーバ型システムにおけるサーバ装置 1 に、サーバ側ローカル保守コンソール 2 からの利用可能時間の設定要求の受付けとクライアント装置 3 への転送の機能を持たせた点と、各クライアント装置 3 に、遠隔保守コンソール 5 からの保守インタフェース 30 の利用時間を管理し、サーバ装置 1 から事前に設定された利用可能時間を超える場合には遠隔保守コンソール 5 に対して利用時間終了通知を送出して強制切断すると共に、利用者認識部 32 に登録されている利用者認証情報を無効化する利用時間管理部 38 を備えている点で、第 4 の実施の形態と相違し、その他

は第4の実施の形態と同じである。

【0109】

図21はサーバ側ローカル保守コンソール2から利用者認証情報設定要求が入力された際のサーバ装置1の処理例を示すフローチャートである。システム管理者等が、利用者認証情報の設定対象となるクライアント装置3の指定情報と、設定したい利用者認証情報としてのユーザ名およびパスワードと、設定したい利用可能時間とを指定した利用者認証情報設定要求をサーバ側ローカル保守コンソール2から入力すると、要求受付部11がこの要求を受信し(S501)、ユーザ名、パスワードおよび利用可能時間の桁数などの正常性をチェックする(S502)。桁数などが所定の条件を満足しない場合、要求は拒否される。問題がなければ、受け付けた利用者認証情報設定要求中のユーザ名およびパスワードを暗号化部13において暗号化し(S503～S505)、暗号化されたユーザ名およびパスワードと利用可能時間を含む利用者認証情報設定要求を要求転送部12へ伝達する(S506)。次に、要求転送部12により、利用者認証情報設定要求中で指定されているクライアント装置3のIPアドレスを取得し(S507)、このIPアドレスを用いて利用者認証情報設定要求中の暗号化されたユーザ名およびパスワードと利用可能時間を含む利用者認証情報設定指示をLAN6経由で対象クライアント装置3へ送信する(S508)。そして、対象クライアント装置3から利用者認証情報設定完了通知が返されてくると、この通知を要求転送部12で受信し、要求受付部11経由でサーバ側ローカル保守コンソール2に利用者認証情報設定完了通知を出力する(S509～S511)。

【0110】

図22はサーバ装置1から利用者認証情報設定指示がLAN6経由で送信されてきた際のクライアント装置3の処理例を示すフローチャートであり、ステップS521、S522、S523が追加されている点が図18のフローチャートと相違する。LAN経由で利用者認証情報設定指示が送信されてきたクライアント装置3は、この指示をリモート要求処理部33で受信し(S121)、この指示中の暗号化されたユーザ名およびパスワードを復号化部36で復号化し(S311～S313)、ユーザ名、パスワードおよび利用可能時間が所定の桁数を満たす

かどうかのチェックを行い（S 1 2 2）、問題がなければ、利用可能時間を利用時間管理部 3 8 に伝達する（S 5 2 1）。利用時間管理部 3 8 は、この利用可能時間を記憶する（S 5 2 2）。他方、リモート要求処理部 3 3 は、ユーザ名およびパスワードを含む利用者認証情報設定指示を利用者認証部 3 2 に伝達する（S 1 2 3）。以降、図 1 8 と同様の処理が行われ（S 4 0 1～S 4 0 5、S 1 2 4、S 1 2 5）、利用者認証情報が利用者認証部 3 2 に記憶されて保守インタフェース 3 0 が開放された時点で、利用時間管理部 3 8 は記憶した利用可能時間に従って、利用時間の管理を開始する（S 5 2 3）。

【0 1 1 1】

図 2 3 は利用時間管理部 3 8 が利用時間の管理を開始した後の処理例を示すフローチャートである。利用時間管理部 3 8 は利用時間の管理を開始すると、内部に記録されている利用可能時間を時間の経過に応じて減算していき、残り利用時間が 0 になったかどうか、つまり事前に設定された利用可能時間が経過したかどうかを判定する（S 5 4 1）。そして、残り利用時間が 0 になると、ログイン中の遠隔保守コンソール 5 が存在する場合（S 5 4 2 で Y E S）、ログイン中の遠隔保守コンソール 5 に対して利用時間終了通知を送信し、強制切断を行う（S 5 4 3）。ログイン中の遠隔保守コンソール 5 が存在しない場合には、このステップ S 5 4 3 はスキップされる。次に利用時間管理部 3 8 は、利用者認証部 3 2 に対して利用者認証情報の無効化を指示し、それに応じて利用者認証部 3 2 が登録されている利用者認証情報を無効化する（S 5 4 4）。その後、利用時間管理部 3 8 が初期化される（S 5 4 5）。

【0 1 1 2】

図 2 4 は本実施の形態の動作例を示すシーケンスチャートであり、以下の 2 つの場面のシーケンスが示されている。

（1）サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用者認証情報および利用可能時間の設定

（2）遠隔保守コンソール 5 によるクライアント装置 3 へのログイン

【0 1 1 3】

以下、上記の 2 つの場面について本実施の形態の動作を説明する。

【0114】

(1) 先ず、図20～図24を参照して、サーバ側ローカル保守コンソール2からクライアント装置3へ利用者認証情報および利用可能時間を設定する際の動作を説明する。

【0115】

システム管理者等が、サーバ側ローカル保守コンソール2から、クライアント装置3の保守インタフェース30のセキュリティを開放するためのユーザ名およびパスワードと、対象とするクライアント装置3の指定と、利用可能時間とを含む利用者認証情報設定要求を入力すると(図24のR501)、サーバ装置1でこの要求の受付処理が行われる(R502)。この受付処理では、要求受付部11が利用者認証情報設定要求を受信する処理とユーザ名、パスワードおよび利用可能時間の正常性をチェックする処理とが行われる(図21のS501、S502)。そして問題がなければ、暗号化部13でユーザ名およびパスワードを暗号化する処理が実施される(図24のR503、図21のS503～S505)。そして、暗号化されたユーザ名およびパスワードならびに利用可能時間を含む利用者認証情報設定要求が要求受付部11から要求転送部11へ伝達される(S506)。その後、要求転送部12は、利用者認証情報設定要求中で指定されたクライアント装置3のIPアドレスを取得し(S507)、LAN6を経由してクライアント装置3のリモート要求処理部33へ暗号化されたユーザ名およびパスワードならびに利用可能時間を含む利用者認証情報設定指示を送信する(図24のR504、図21のS508)。

【0116】

クライアント装置3は、サーバ装置1から転送されてきた利用者認証情報設定指示をリモート要求処理部33で受信し(図22のS121)、指示中に含まれる暗号化されたユーザ名およびパスワードを復号化部36を用いて復号化する(図24のR505、図22のS311～S313)。続いて、復号化されたユーザ名およびパスワードならびに利用可能時間の正常性を確認し(S122)、問題がなければ、先ず利用可能時間を利用時間管理部38に伝達する(S521)。利用時間管理部38はこの利用可能時間を記憶する(図24のR506、図22

の S 5 2 2)。次にリモート要求処理部 3 3 は、ユーザ名およびパスワードを含む利用者認証情報設定指示を利用者認証部 3 2 に伝達する (S 1 2 3)。以降、図 1 8 を参照して説明した処理と同様の処理が行われ (S 4 0 1 ~ S 4 0 5、S 1 2 4、S 1 2 5)、利用者認証部 3 2 にユーザ名とパスワードが設定され (図 2 4 の R 5 0 7)、また利用者認証情報設定完了通知がクライアント装置 3 からサーバ側リモート保守コンソール 2 へ通知される (R 5 0 8、R 5 0 9)。そして、利用時間管理部 3 8 が利用時間の管理を開始する (R 5 1 0、図 2 2 の S 5 2 3)。

【0 1 1 7】

(2) 次に、遠隔保守コンソール 5 から何者かがクライアント装置 3 へログインしたときの動作を、図 2 3 および図 2 4 を参照して説明する。

【0 1 1 8】

クライアント装置 3 の利用者認証部 3 2 にユーザ名およびパスワードが設定され、また利用時間管理部 3 8 で利用時間の管理が開始された後、何者かが遠隔保守コンソール 5 から LAN 6 経由でクライアント装置 3 に対してユーザ名およびパスワードを指定したログイン要求を入力すると (図 2 4 の R 5 1 1)、図 8 および図 1 0 を参照して説明した処理と同様の処理がクライアント装置 3 で実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部 3 2 に登録されているユーザ名およびパスワードと一致すると、ログインが許可され (図 2 4 の R 5 1 2、R 5 1 3)、遠隔保守コンソール 5 からクライアント装置 3 の保守対象部 3 1 に対するアクセスが可能となる。

【0 1 1 9】

しかし、遠隔保守コンソール 5 からログイン・ログアウト処理部 3 5 に対してログアウト要求が入力される前に利用可能時間が経過した場合 (図 2 4 の R 5 1 5、図 2 3 の S 5 4 1 および S 5 4 2 で Y E S)、利用時間管理部 3 5 は、遠隔保守コンソール 5 に対して利用時間終了通知を送信し、強制切断を行う (図 2 4 の R 5 1 6、図 2 3 の S 5 4 3)。また利用時間管理部 3 8 は、利用者認証部 3 2 に対して利用者認証情報の無効化を指示し、利用者認証部 3 2 は登録されている利用者認証情報を無効化する (図 2 4 の R 5 1 7、図 2 3 の S 5 4 4)。

【0120】

以上説明したように本実施の形態によれば、サーバ側ローカル保守コンソール 2 から利用可能時間を指定して、クライアント装置 3 の保守インタフェース 30 の利用時間を管理することができる。従って、クライアント装置 3 の保守インタフェース 30 が一度開放された後、保守インタフェース 30 が長時間開放し続け、悪意のアクセスの危険性が高くなることを防ぐことができる。

【0121】

なお、本実施の形態では、サーバ側ローカル保守コンソール 2 からクライアント装置 3 に利用者認証情報を設定する指示で利用可能時間を併せて設定するように指示したが、サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用者認証情報の設定指示と、サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用可能時間の設定指示とを独立させるようにしても良い。また、サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用可能時間の設定機能を無くし、利用時間管理部 38 に予め記憶された固定の利用可能時間を使用するようにしても良い。

【0122】

また、本実施の形態において、第 1 の実施の形態と同様にそれぞれのクライアント装置 3 に図 1 のクライアント側ローカル保守コンソール 4 を接続し、クライアント装置 3 内にローカル要求処理部 34 を設けるようにしても良い。さらに、利用者認証情報を暗号化せずにサーバ装置 1 からクライアント装置 3 へ転送するようにしても良く、その場合には暗号化部 13 および復号化部 36 は省略される。また、利用者認証情報の再設定時にログイン中の遠隔保守コンソール 5 を強制切断しないようにしても良く、その場合には強制切断部 37 は省略される。

【0123】**【発明の第 6 の実施の形態】**

図 25 を参照すると、本発明の第 6 の実施の形態にかかるクライアント・サーバ型システムは、図 20 に示した第 5 の実施の形態にかかるクライアント・サーバ型システムにおけるサーバ装置 1 に、サーバ側ローカル保守コンソール 2 からのログイン可能回数の要求の受け付けとクライアント装置 3 への転送の機能を持た

せた点と、各クライアント装置 3 に、遠隔保守コンソール 5 からのログイン回数を管理し、サーバ装置 1 から設定されたログイン可能回数を超過した場合にはログインを許可せず遠隔保守コンソール 5 に対して利用回数終了通知を送出すると共に、利用者認識部 3 2 に登録されている利用者認証情報を無効化するログイン回数管理部 3 9 を備えている点で、第 5 の実施の形態と相違し、その他は第 5 の実施の形態と同じである。

【 0 1 2 4 】

図 2 6 はサーバ側ローカル保守コンソール 2 から利用者認証情報設定要求が入力された際のサーバ装置 1 の処理例を示すフローチャートである。システム管理者等が、利用者認証情報の設定対象となるクライアント装置 3 の指定情報と、設定したい利用者認証情報としてのユーザ名およびパスワードと、設定したい利用可能時間と、設定したいログイン可能回数とを指定した利用者認証情報設定要求をサーバ側ローカル保守コンソール 2 から入力すると、要求受付部 1 1 がこの要求を受信し（S 6 0 1）、ユーザ名、パスワード、利用可能時間およびログイン可能回数の桁数などの正常性をチェックする（S 6 0 2）。桁数などが所定の条件を満足しない場合、要求は拒否される。問題がなければ、受け付けた利用者認証情報設定要求中のユーザ名およびパスワードを暗号化部 1 3 において暗号化し（S 6 0 3 ～ S 6 0 5）、暗号化されたユーザ名およびパスワードと利用可能時間ならびにログイン可能回数を含む利用者認証情報設定要求を要求転送部 1 2 へ伝達する（S 6 0 6）。次に、要求転送部 1 2 により、利用者認証情報設定要求中で指定されているクライアント装置 3 の IP アドレスを取得し（S 6 0 7）、この IP アドレスを用いて利用者認証情報設定要求中の暗号化されたユーザ名およびパスワードと利用可能時間ならびにログイン可能回数を含む利用者認証情報設定指示を LAN 6 経由で対象クライアント装置 3 へ送信する（S 6 0 8）。そして、対象クライアント装置 3 から利用者認証情報設定完了通知が返されてくると、この通知を要求転送部 1 2 で受信し、要求受付部 1 1 経由でサーバ側ローカル保守コンソール 2 に利用者認証情報設定完了通知を出力する（S 6 0 9 ～ S 6 1 1）。

【 0 1 2 5 】

図 27 はサーバ側ローカル保守コンソール 2 から利用者認証情報設定要求が入力された際のサーバ装置 1 の処理例を示すフローチャートであり、ステップ S 6 2 1、S 6 2 2 が追加されている点が図 22 のフローチャートと相違する。LAN 経由で利用者認証情報設定指示が送信されてきたクライアント装置 3 は、この指示をリモート要求処理部 33 で受信すると (S 1 2 1)、この指示中の暗号化されたユーザ名およびパスワードを復号化部 36 で復号化し (S 3 1 1 ~ S 3 1 3)、ユーザ名、パスワード、利用可能時間およびログイン可能回数が所定の桁数を満たすかどうかのチェックを行う (S 1 2 2)。問題がなければ、利用可能時間を利用時間管理部 38 に伝達し (S 5 2 1)、利用時間管理部 38 はこの利用可能時間を記憶する (S 5 2 2)。さらに、ログイン可能回数をログイン回数管理部 39 に伝達し (S 6 2 1)、ログイン回数管理部 39 はこのログイン可能回数を記憶する (S 6 2 2)。以降、図 22 と同様の処理が行われる (S 1 2 3、S 4 0 1 ~ S 4 0 5、S 1 2 4、S 1 2 5、S 5 2 3)。

【0126】

図 28 は遠隔保守コンソール 5 からユーザ名およびパスワードの指定を含むログイン要求が LAN 6 経由で送信されてきた際のクライアント装置 3 の処理例を示すフローチャートであり、ステップ S 6 3 1 ~ S 6 3 5 が追加されている点が図 8 のフローチャートと相違する。本実施の形態においては、ログイン・ログアウト処理部 35 で遠隔保守コンソール 5 からのログイン要求を受信すると (S 1 6 1)、ログイン回数管理部 39 でログイン回数を +1 し (S 6 3 1)、事前に設定されたログイン可能回数を超えたかどうかを判定する (S 6 3 2)。ログイン可能回数を超えていない場合は図 8 と同様の処理が行われる (S 1 6 2 ~ S 1 7 2)。

【0127】

他方、ログイン回数がログイン可能回数を超えていた場合は、ログイン回数管理部 39 からログイン要求を出した遠隔保守コンソール 5 に対して利用回数終了通知を送出する (S 6 3 3)。このときログイン・ログアウト処理部 35 はログイン許可を与えない。さらに利用者認証部 32 は、登録されている利用者認証情報を無効化する (S 6 3 4)。そして、ログイン回数管理部 38 が初期化される (

S 6 3 5)。

【0 1 2 8】

図 2 9 は本実施の形態の動作例を示すシーケンスチャートであり、以下の 2 つの場面のシーケンスが示されている。

(1) サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用者認証情報および利用可能時間ならびにログイン可能回数の設定

(2) 遠隔保守コンソール 5 からのクライアント装置 3 への頻繁なログイン

【0 1 2 9】

以下、上記の 2 つの場面について本実施の形態の動作を説明する。

【0 1 3 0】

(1) 先ず、図 2 5 ～図 2 7 および図 2 9 を参照して、サーバ側ローカル保守コンソール 2 からクライアント装置 3 へ利用者認証情報、利用可能時間およびログイン可能回数を設定する際の動作を説明する。

【0 1 3 1】

システム管理者等が、サーバ側ローカル保守コンソール 2 から、クライアント装置 3 の保守インタフェース 3 0 のセキュリティを開放するためのユーザ名およびパスワードと、対象とするクライアント装置 3 の指定と、許容するログイン最大時間である利用可能時間と、この利用可能時間内における最大ログイン可能回数であるログイン可能回数とを含む利用者認証情報設定要求を入力すると (図 2 9 の R 6 0 1)、サーバ装置 1 でこの要求の受付処理が行われる (R 6 0 2)。この受付処理では、要求受付部 1 1 が利用者認証情報設定要求を受信する処理とユーザ名、パスワード、利用可能時間およびログイン可能回数の正常性をチェックする処理とが行われる (図 2 6 の S 6 0 1、S 6 0 2)。そして問題がなければ、暗号化部 1 3 でユーザ名およびパスワードを暗号化する処理が実施される (図 2 9 の R 6 0 3、図 2 6 の S 6 0 3 ～S 6 0 5)。そして、暗号化されたユーザ名およびパスワードと利用可能時間およびログイン可能回数を含む利用者認証情報設定要求が要求受付部 1 1 から要求転送部 1 1 へ伝達される (S 6 0 6)。その後、要求転送部 1 2 は、利用者認証情報設定要求中で指定されたクライアント装置 3 の I P アドレスを取得し (S 6 0 7)、L A N 6 を経由してクライアント

装置 3 のリモート要求処理部 33 へ暗号化されたユーザ名およびパスワードならびに利用可能時間を含む利用者認証情報設定指示を送信する（図 29 の R604、図 26 の S608）。

【0132】

クライアント装置 3 は、サーバ装置 1 から転送されてきた利用者認証情報設定指示をリモート要求処理部 33 で受信し（図 27 の S121）、指示中に含まれる暗号化されたユーザ名およびパスワードを復号化部 36 を用いて復号化する（図 29 の R605、図 27 の S311～S313）。続いて、復号されたユーザ名およびパスワードと利用可能時間およびログイン可能回数の正常性を確認し（S122）、問題がなければ、利用可能時間を利用時間管理部 38 に、ログイン可能回数をログイン回数管理部 39 にそれぞれ伝達し、利用時間管理部 38 が利用可能時間を、ログイン回数管理部 39 がログイン可能回数をそれぞれ記憶する（図 29 の R606、図 27 の S521、S522、S621、S622）。次にリモート要求処理部 33 は、ユーザ名およびパスワードを含む利用者認証情報設定指示を利用者認証部 32 に伝達する（S123）。以降、図 22 と同様の処理が行われ（S401～S405、S124、S125、S523）、利用者認証部 32 にユーザ名とパスワードが設定され（図 29 の R607）、また利用者認証情報設定完了通知がクライアント装置 3 からサーバ側リモート保守コンソール 2 へ通知される（R608、R609）。さらに、利用時間管理部 38 が利用時間の管理を開始する（R610）。

【0133】

（2）次に、遠隔保守コンソール 5 から保守作業者がクライアント装置 3 へ頻繁にログインしたときの動作を、図 25、図 28 および図 29 を参照して説明する。

【0134】

クライアント装置 3 の利用者認証部 32 にユーザ名およびパスワードが設定され、利用時間管理部 38 に利用可能時間が設定され、さらにログイン回数管理部 39 にログイン可能回数が設定された後、何者かが遠隔保守コンソール 5 から LAN 6 経由でクライアント装置 3 に対してユーザ名およびパスワードを指定したロ

ログイン要求を入力すると（図 29 の R 6 1 1）、ログイン回数管理部 39 でログイン回数が更新され（図 29 の R 6 1 2、図 28 の S 6 3 1）、また利用者認証処理 R 6 1 3 が実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部 32 に登録されているユーザ名およびパスワードと一致すると、ログインが許可される（図 29 の R 6 1 4）。これにより、遠隔保守コンソール 5 からクライアント装置 3 の保守対象部 31 に対するアクセスが可能となる。その後、図 30 のシーケンスでは、遠隔保守コンソールがログアウトし、再びログインしている。

【0135】

第 5 の実施の形態では利用可能時間以内であれば遠隔保守コンソール 5 からユーザ名およびパスワードを使ってログイン、ログアウトを何度も繰り返すことができた。しかし、本実施の形態の場合、ログイン要求がある毎にログイン回数管理部 39 がログイン回数を更新し、ログイン回数が事前に設定されたログイン可能回数を超えると（図 29 の R 6 2 1、図 28 の S 6 3 2 で YES）、利用可能時間が終了する前であっても、利用回数終了通知を遠隔保守コンソール 5 へ通知し（図 29 の R 6 2 2、図 28 の S 6 3 3）、ログインを許可しない。また、利用者認証部 32 は登録されているユーザ名およびパスワードを無効とする（図 29 の R 6 2 3、図 28 の S 6 3 4）。

【0136】

このように本実施の形態によれば、クライアント装置 3 の保守インタフェース 30 の利用回数（ログイン回数）を管理することができる。従って、クライアント装置 3 の保守インタフェース 30 が一度開放された後、保守インタフェース 30 が頻繁にアタックされるのを防ぐことができ、クライアント装置 3 が輻輳することを防ぐことができる。

【0137】

なお、本実施の形態では、サーバ側ローカル保守コンソール 2 からクライアント装置 3 に利用者認証情報を設定する指示でログイン可能回数を併せて設定するように指示したが、サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用者認証情報の設定指示と、サーバ側ローカル保守コンソール 2 からクライ

アント装置 3 へのログイン可能回数の設定指示とを独立させるようにしても良い。また、サーバ側ローカル保守コンソール 2 からクライアント装置 3 へのログイン可能回数の設定機能無くし、ログイン回数管理部 39 に予め記憶された固定のログイン可能回数を使用するようにしても良い。

【0138】

また、本実施の形態において、第 1 の実施の形態と同様にそれぞれのクライアント装置 3 に図 1 のクライアント側ローカル保守コンソール 4 を接続し、クライアント装置 3 内にローカル要求処理部 34 を設けるようにしても良い。さらに、利用者認証情報を暗号化せずにサーバ装置 1 からクライアント装置 3 へ転送するようにしても良く、その場合には暗号化部 13 および復号化部 36 は省略される。また、利用者認証情報の再設定時にログイン中の遠隔保守コンソール 5 を強制切断しないようにしても良く、その場合には強制切断部 37 は省略される。さらに、利用可能時間を管理しないようにしても良く、その場合には利用時間管理部 38 は省略される。

【0139】

【発明の第 7 の実施の形態】

図 30 を参照すると、本発明の第 7 の実施の形態にかかるクライアント・サーバ型システムは、図 25 に示した第 6 の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置 3 に、利用可能時間基準値 3A-1 およびログイン可能回数基準値 3A-2 を予め記憶する手段を備え、遠隔保守コンソール 5 からの利用者認証情報設定指示中に利用可能時間、ログイン可能回数が含まれていないか、含まれていても受信不良等で使用できない場合に、利用可能時間基準値 3A-1 およびログイン可能回数基準値 3A-2 を利用時間管理部 38 およびログイン回数管理部 39 に設定するようにした点で、第 6 の実施の形態と相違し、その他は第 6 の実施の形態と同じである。

【0140】

図 31 はサーバ側ローカル保守コンソール 2 から利用者認証情報設定要求が入力された際のサーバ装置 1 の処理例を示すフローチャートである。システム管理者等は、利用者認証情報の設定対象となるクライアント装置 3 の指定情報と、設定

したい利用者認証情報としてのユーザ名およびパスワードと、設定したい利用可能時間と、設定したいログイン可能回数とを指定した利用者認証情報設定要求をサーバ側ローカル保守コンソール 2 から入力する。本実施の形態の場合、利用可能時間およびログイン可能回数の指定は任意であり、クライアント装置 3 の利用可能時間基準値 3 A-1、ログイン可能回数基準値 3 A-2 を利用する場合には指定する必要はない。サーバ側ローカル保守コンソール 2 からの上記要求は、要求受付部 11 で受信され (S701)、以下、図 26 のステップ S602~S611 と同様な処理が行われる (S702~S711)。

【0141】

図 32 はサーバ装置 1 から利用者認証情報設定指示が LAN 6 経由で送信されてきた際のクライアント装置 3 の処理例を示すフローチャートであり、図 27 のステップ S521、S522、S621、S622 の部分がステップ S701~S708 に置き換えられている点が図 27 のフローチャートと相違する。LAN 経由で利用者認証情報設定指示が送信されてきたクライアント装置 3 は、この指示をリモート要求処理部 33 で受信すると (S121)、この指示中の暗号化されたユーザ名およびパスワードを復号化部 36 で復号化し (S311~S313)、ユーザ名およびパスワードについて、また若し含まれていれば利用可能時間およびログイン可能回数について、所定の桁数を満たすかどうか等のチェックを行う (S122)。利用可能時間が含まれており利用可能ならば (S701 で YES)、それを利用時間管理部 38 に伝達し (S702)、利用可能時間が含まれていないか或いは受信不良で使えない場合には (S701 で NO)、利用可能時間基準値 3 A-1 を利用時間管理部 38 に伝達する (S703)。利用時間管理部 38 はこの伝達された利用可能時間を記憶する (S704)。さらに、リモート要求処理部 33 は、ログイン可能回数が指示中に含まれており利用可能ならば (S705 で YES)、それをログイン回数管理部 39 に伝達し (S706)、ログイン可能回数が含まれていないか或いは受信不良で使えない場合には (S705 で NO)、ログイン可能回数基準値 3 A-2 をログイン回数管理部 39 に伝達する (S707)。ログイン回数管理部 39 はこの伝達されたログイン可能回数を記憶する (S708)。以降、図 27 の場合と同様な処理が行われる (S1

23、S401～S405、S124、S125、S523)。

【0142】

本実施の形態によれば、サーバ側ローカル保守コンソール2からクライアント装置3に利用者認証情報を設定して保守インタフェース30を開放するに際し、サーバ側ローカル保守コンソール2から利用可能時間が設定されない場合にも、クライアント装置3の利用可能時間基準値3A-1を用いて利用時間を管理でき、利用可能時間基準値3A-1を超えた場合に保守インタフェース30の利用を強制的に禁止することができる。従って、利用可能時間が指定されずにクライアント装置3の保守インタフェース30が開放された場合も、保守インタフェース30が長時間開放し続け、悪意のアクセスの危険性が高くなることを防ぐことができる。

【0143】

また本実施の形態によれば、サーバ側ローカル保守コンソール2からクライアント装置3に利用者認証情報を設定して保守インタフェース30を開放するに際し、サーバ側ローカル保守コンソール2からログイン可能回数が設定されない場合にも、クライアント装置3のログイン可能回数基準値3A-2を用いてログイン回数を管理でき、ログイン回数がログイン可能回数基準値3A-2を超えた場合に保守インタフェース30の利用を強制的に禁止することができる。従って、ログイン可能回数が指定されずにクライアント装置3の保守インタフェース30が開放された場合にも、保守インタフェース30が多数回アタックされるのを防ぐことができる。

【0144】

なお、本実施の形態において、第1の実施の形態と同様にそれぞれのクライアント装置3に図1のクライアント側ローカル保守コンソール4を接続し、クライアント装置3内にローカル要求処理部34を設けるようにしても良い。また、利用者認証情報を暗号化せずにサーバ装置1からクライアント装置3へ転送するようにしても良く、その場合には暗号化部13および復号化部36は省略される。さらに、利用者認証情報の再設定時にログイン中の遠隔保守コンソール5を強制切断しないようにしても良く、その場合には強制切断部37は省略される。

【0145】

【発明の第8の実施の形態】

図33を参照すると、本発明の第8の実施の形態にかかるクライアント・サーバ型システムは、図30に示した第7の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置3に、保守インタフェース30を開放してから初回のログインに限り、利用時間管理部38における残り利用時間を予め定められた延長時間だけ延長する利用時間延長部3Bを備えている点で、第7の実施の形態と相違し、その他は第7の実施の形態と同じである。

【0146】

図34(A)は利用時間延長部3Bの処理例を示すフローチャートである。利用時間延長部3Bは、たとえば利用時間管理部38と同時に起動される。利用時間管理部38は、先ず、利用者認証部32に利用者認証情報が設定されることで保守インタフェース30が開放されてから、初めて遠隔保守コンソール5のログインが行われたかどうかを検出する(S801)。これは、例えばログイン回数管理部34で管理されているログイン回数が1になったかどうかを検出することで可能である。遠隔保守コンソール5からの初回のログインを検出すると、利用時間延長部3Bは、利用時間管理部38で管理されている利用時間の残り時間が予め設定された時間以下であるかどうかを検出する(S802)。そして、残り利用時間が予め設定された時間以下であれば(S802でYES)、利用時間管理部38で管理されている残り時間情報に、予め定められた延長時間を加算する(S803)。加算せずに延長時間だけを残り時間として再設定しても良い。他方、初回のログイン時点における残り利用時間が予め設定された時間以下でなければ(S802でNO)、もはや利用時間の延長処理を行わないため、図34(A)の処理を終了する。

【0147】

図35は本実施の形態の動作例を示すシーケンスチャートであり、以下の2つの場面のシーケンスが示されている。

(1) サーバ側ローカル保守コンソール2からクライアント装置3への利用者認証情報および利用可能時間ならびにログイン可能回数の設定

(2) 遠隔保守コンソール 5 からのクライアント装置 3 への初回のログイン

【0148】

(1) のシーケンスにおける本実施の形態の動作は図 29 のシーケンスの場合と同じであるので、以下では遠隔保守コンソール 5 から保守作業者がクライアント装置 3 へ初めてログインした場面 (2) の動作を、図 33～図 35 を参照して説明する。

【0149】

クライアント装置 3 の利用者認証部 32 にユーザ名およびパスワードが設定され、利用時間管理部 38 に利用可能時間が設定され、さらにログイン回数管理部 39 にログイン可能回数が設定された後、暫く経って、保守作業者が遠隔保守コンソール 5 から LAN 6 経由でクライアント装置 3 に対してユーザ名およびパスワードを指定したログイン要求を入力すると (図 35 の R801)、ログイン回数管理部 39 でログイン回数が更新され (図 35 の R802)、ログイン回数=1 となる。また利用者認証処理 R803 が実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部 32 に登録されているユーザ名およびパスワードと一致すると、ログインが許可される (図 35 の R804)。これにより、遠隔保守コンソール 5 からクライアント装置 3 の保守対象部 31 に対するアクセスが可能となる。

【0150】

利用者認証部 32 に利用者認証情報が設定され保守インタフェース 30 が開放されてから遠隔保守コンソールがログインするまでに暫く時間が空いていたため、ログインした時点で利用時間の残り時間が予め定められた時間以下であった場合 (図 35 の R805)、そのことが利用時間延長部 3B で検出され (図 34 (A) の S802 で YES)、利用時間管理部 33 の残り利用時間に予め定められた延長時間が加算される (図 35 の R806、図 34 (A) の S803)。その後、図 35 のシーケンスでは、保守作業者が保守作業を終えたので、遠隔保守コンソール 5 をログアウトしている (R807～R809)。

【0151】

このように本実施の形態によれば、サーバ側ローカル保守コンソール 2 からクラ

クライアント装置 3 の保守インタフェース 30 を時間設定して開放した後、遠隔保守コンソール 5 からの初回のログインが利用時間終了近くで実行された場合に、十分な保守作業を行わせることを目的として、一定時間の利用時間延長を行うことができる。従って、何らかの理由で初回のログインが遅れた場合でも保守作業を支障なく行うことが可能となる。なお、図 34 (A) の処理では、初回のログイン時点における残り利用時間が所定時間以下であった場合に利用時間の延長を認めたが、初回のログイン時点における残り利用時間が所定時間以上あっても、保守作業に時間がかかったため残り利用時間が足りなくなった場合に利用時間を延長するようにしても良い。図 34 (B) はこのような実施の形態における利用時間延長部 3 B の処理例を示すフローチャートであり、図 34 (A) のフローチャートにステップ S 804 が追加されている。利用時間管理部 38 は、利用者認証部 32 に利用者認証情報が設定されることで保守インタフェース 30 が開放されてから、初めて遠隔保守コンソール 5 のログインが行われたことを検出すると (S 801)、利用時間管理部 38 で管理されている利用時間の残り時間が予め設定された時間以下であるかどうか (S 802)、初回のログインが継続中であるかどうか (S 803) をそれぞれ検出する。初回のログインが継続中であるかどうかはログイン・ログアウト処理部 35 で管理されているログイン状態を参照することで検出できる。そして、初回のログイン中に利用時間の残り時間が予め定められた時間以下になっていることを検出すると (S 802 で YES)、利用時間管理部 38 で管理されている残り時間情報に、予め定められた延長時間を加算する (S 803)。加算せずに延長時間だけを残り時間として再設定しても良い。他方、初回のログインが終了し、遠隔保守コンソール 5 がログアウトした場合 (S 804 で NO)、もはや利用時間の延長処理を行わないため、図 34 (B) の処理を終了する。

【0152】

なお、本実施の形態において、第 1 の実施の形態と同様にそれぞれのクライアント装置 3 に図 1 のクライアント側ローカル保守コンソール 4 を接続し、クライアント装置 3 内にローカル要求処理部 34 を設けるようにしても良い。さらに、利用者認証情報を暗号化せずにサーバ装置 1 からクライアント装置 3 へ転送するよ

うにしても良く、その場合には暗号化部 1 3 および復号化部 3 6 は省略される。
また、利用者認証情報の再設定時にログイン中の遠隔保守コンソール 5 を強制切断しないようにしても良く、その場合には強制切断部 3 7 は省略される。さらに、ログイン可能回数を管理しないようにしても良く、その場合にはログイン回数管理部 3 9 は省略される。この場合、保守インタフェース 3 0 開放後の初回のログインかどうかは、例えば利用時間延長部 3 B 内で保守インタフェース 3 0 開放後のログイン回数を管理することで可能である。

【 0 1 5 3 】

【発明の第 9 の実施の形態】

図 3 6 を参照すると、本発明の第 9 の実施の形態にかかるクライアント・サーバ型システムは、図 3 3 に示した第 8 の実施の形態にかかるクライアント・サーバ型システムにおける各クライアント装置 3 に、ログイン中の遠隔保守コンソール 5 から保守インタフェース利用終了通知を受信したときに利用者認証部 3 2 に登録されている利用者認証情報を無効化し、利用者認証情報を無効化した旨の通知を遠隔保守コンソール 5 に送信する認証無効化部 3 C を備えている点で、第 8 の実施の形態と相違し、その他は第 8 の実施の形態と同じである。

【 0 1 5 4 】

図 3 7 は本実施の形態の動作例を示すシーケンスチャートであり、以下の 2 つの場面のシーケンスが示されている。

(1) サーバ側ローカル保守コンソール 2 からクライアント装置 3 への利用者認証情報および利用可能時間ならびにログイン可能回数の設定

(2) 遠隔保守コンソール 5 からのクライアント装置 3 へのログインと保守インタフェース利用終了通知の送出

【 0 1 5 5 】

(1) のシーケンスにおける本実施の形態の動作は図 2 9 のシーケンスの場合と同じであるので、以下では遠隔保守コンソール 5 から保守作業者がクライアント装置 3 へログインして保守作業を行い、保守作業の終了時に保守インタフェース利用終了通知を遠隔保守コンソール 5 から入力した場面 (2) の動作を、図 3 6 および図 3 7 を参照して説明する。

【0156】

クライアント装置3の利用者認証部32にユーザ名およびパスワードが設定され、利用時間管理部38に利用可能時間が設定され、さらにログイン回数管理部39にログイン可能回数が設定された後、保守作業者が遠隔保守コンソール5からLAN6経由でクライアント装置3に対してユーザ名およびパスワードを指定したログイン要求を入力すると（図37のR901）、ログイン回数管理部39でログイン回数が更新され（図37のR902）、また利用者認証処理R903が実施され、ログイン要求中のユーザ名およびパスワードが利用者認証部32に登録されているユーザ名およびパスワードと一致すると、ログインが許可される（図37のR904）。これにより、遠隔保守コンソール5からクライアント装置3の保守対象部31に対するアクセスが可能となる。

【0157】

保守作業者がクライアント装置3の保守対象部31に対する保守を終え、遠隔保守コンソール5から保守インタフェース利用終了通知を入力すると（R905）、それがクライアント装置3のログイン・ログアウト処理部35を通じて認証無効化部3Cに伝達される。認証無効化部3Cは、利用者認証部32に対して利用者認証情報の無効化を指示し、利用者認証部32はそれに応じて、登録されている利用者認証情報を消去する等して無効にする（R906）。その後、認証無効化3Cは、遠隔保守コンソール5に対して利用者認証情報無効化通知を送出する（R907）。以後、保守インタフェース30は再度開放されるまで閉塞され、その利用は不可能となる。

【0158】

このように本実施の形態によれば、サーバ側ローカル保守コンソール2からクライアント装置3の保守インタフェース30を時間設定して開放した後、遠隔保守コンソール5からログインして保守作業を行い、その終了時に遠隔保守コンソール5側から保守インタフェース利用終了通知を入力することにより、利用時間終了前であってもクライアント装置3の保守インタフェース30を利用禁止とすることができる。このように保守作業終了とともに利用者認証情報を無効化できるようにしたことにより、保守インタフェース30が長時間開放し続け、悪意のア

クセスの危険性が高くなることを防ぐことができる。

【0159】

なお、本実施の形態において、第1の実施の形態と同様にそれぞれのクライアント装置3に図1のクライアント側ローカル保守コンソール4を接続し、クライアント装置3内にローカル要求処理部34を設けるようにしても良い。さらに、利用者認証情報を暗号化せずにサーバ装置1からクライアント装置3へ転送するようにしても良く、その場合には暗号化部13および復号化部36は省略される。また、利用者認証情報の再設定時にログイン中の遠隔保守コンソール5を強制切断しないようにしても良く、その場合には強制切断部37は省略される。さらに、利用時間を延長しないようにしても良く、その場合には利用時間延長部3Bは省略される。また利用可能時間を管理しないようにしても良く、その場合には利用時間管理部38および利用時間延長部3Bは省略される。また、ログイン可能回数を管理しないようにしても良く、その場合にはログイン回数管理部39は省略される。

【0160】

以上本発明の実施の形態について説明したが、本発明は以上の実施の形態にのみ限定されず、その他各種の付加変更が可能である。例えば、サーバ装置1とクライアント装置とを接続するネットワークは、LANに限られず、インターネットやイントラネット等の他の種類のネットワークであっても良い。

【0161】

本発明のサーバ装置およびクライアント装置は、その有する機能をハードウェア的に実現することは勿論、コンピュータとサーバプログラム、クライアントプログラムとで実現することができる。サーバプログラム、クライアントプログラムは、磁気ディスクや半導体メモリ等のコンピュータ可読記録媒体に記録されて提供され、サーバ装置を構成するコンピュータ、クライアント装置を構成するコンソールの立ち上げ時などにコンピュータに読み取られ、そのコンピュータの動作を制御することにより、そのコンピュータを前述した各実施の形態におけるサーバ装置、クライアント装置として機能させる。

【0162】

【発明の効果】

以上説明したように本発明によれば、以下のような効果が得られる。

【0163】

クライアント・サーバ型分散システムにおいて複数のクライアント装置の保守インタフェースに対するセキュリティ確保のための利用者認証情報の設定および無効化を、サーバ側コンソールから遠隔で制御でき、セキュリティの確保と保守の容易性を両立させることが可能となる。

【0164】

サーバ装置からクライアント装置にネットワークを通じて転送される利用者認証情報を暗号化したため、より強固なセキュリティを実現することができる。

【0165】

利用者認証情報がクライアント装置に設定された後これらが有効である時間、即ち、保守インタフェースの利用可能時間を導入し、利用可能時間経過後に自動的に利用者認証情報を無効にすることにより、保守インタフェースが長時間にわたって開放され続け、悪意のアクセスの危険性が高まることを防ぐことができる。特に、サーバ装置から利用可能時間が指定された場合にはそれを使用し、指定されない場合にはクライアント側に記憶されている利用可能時間基準値を使用する構成にあっては、システム管理者の選択によって利用可能時間を自由に決定することができると共に、指定忘れなどの場合があっても保守インタフェースが長時間にわたって開放し続け、悪意のアクセスの危険性が高まるのを防ぐことができる。

【0166】

初回のログインに限って利用可能時間の延長を自動的に行うようにしたことにより、セキュリティを確保しつつ、ログインするのが遅れた保守作業による保守作業を支障なく行わせることができる。

【0167】

保守インタフェースが開放されてからのログイン回数が所定のログイン可能回数に達すると、ログイン中のアクセスを停止させ、利用者認証情報を無効化するため、ログイン、ログアウトを頻繁に繰り返す悪意の者からの頻繁なアタックを防

止でき、セキュリティを確保することができる。

【0168】

保守作業を終了した保守者から入力された保守インタフェース利用終了通知に連動して、利用者認証情報を自動的に無効化するため、保守インタフェースが長時間にわたって開放され続け、悪意のアクセスの危険性が高まるのを防ぐことができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図2】

本発明の第1の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図3】

本発明の第1の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定無効要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図4】

本発明の第1の実施の形態におけるサーバ装置から利用者認証情報設定指示がLAN経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図5】

本発明の第1の実施の形態におけるサーバ装置から利用者認証情報設定無効指示がLAN経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図6】

本発明の第1の実施の形態におけるクライアント側ローカル保守コンソールから利用者認証情報設定指示が入力された際のクライアント装置の処理例を示すフロ

ーチャートである。

【図 7】

本発明の第 1 の実施の形態におけるクライアント側ローカル保守コンソールから利用者認証情報設定無効要求が入力された際のクライアント装置の処理例を示すフローチャートである。

【図 8】

本発明の第 1 の実施の形態における遠隔保守コンソールからユーザ名およびパスワードの指定を含むログイン要求が LAN 経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図 9】

本発明の第 1 の実施の形態におけるログイン中の遠隔保守コンソールからログアウト要求が LAN 経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図 1 0】

本発明の第 1 の実施の形態の動作例を示すシーケンスチャートである。

【図 1 1】

本発明の第 1 の実施の形態の動作例を示すシーケンスチャートである。

【図 1 2】

本発明の第 2 の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図 1 3】

本発明の第 3 の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図 1 4】

本発明の第 3 の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図 1 5】

本発明の第 3 の実施の形態におけるサーバ装置から利用者認証情報設定指示が L

A N 経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図 1 6】

本発明の第 3 の実施の形態の動作例を示すシーケンスチャートである。

【図 1 7】

本発明の第 4 の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図 1 8】

本発明の第 4 の実施の形態におけるサーバ装置から利用者認証情報設定指示が L A N 経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図 1 9】

本発明の第 4 の実施の形態の動作例を示すシーケンスチャートである。

【図 2 0】

本発明の第 5 の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図 2 1】

本発明の第 5 の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図 2 2】

本発明の第 5 の実施の形態におけるサーバ装置から利用者認証情報設定指示が L A N 経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図 2 3】

本発明の第 5 の実施の形態における利用時間管理部が利用時間の管理を開始した後の処理例を示すフローチャートである。

【図 2 4】

本発明の第 5 の実施の形態の動作例を示すシーケンスチャートである。

【図 2 5】

本発明の第 6 の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図 2 6】

本発明の第 6 の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図 2 7】

本発明の第 6 の実施の形態におけるサーバ装置から利用者認証情報設定指示が LAN 経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図 2 8】

本発明の第 6 の実施の形態における遠隔保守コンソールからユーザ名およびパスワードの指定を含むログイン要求が LAN 経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図 2 9】

本発明の第 6 の実施の形態の動作例を示すシーケンスチャートである。

【図 3 0】

本発明の第 7 の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図 3 1】

本発明の第 7 の実施の形態におけるサーバ側ローカル保守コンソールから利用者認証情報設定要求が入力された際のサーバ装置の処理例を示すフローチャートである。

【図 3 2】

本発明の第 7 の実施の形態におけるサーバ装置から利用者認証情報設定指示が LAN 経由で送信されてきた際のクライアント装置の処理例を示すフローチャートである。

【図 3 3】

本発明の第 8 の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図 3 4】

本発明の第 8 の実施の形態における利用時間延長部の処理例を示すフローチャートである。

【図 3 5】

本発明の第 8 の実施の形態の動作例を示すシーケンスチャートである。

【図 3 6】

本発明の第 8 の実施の形態にかかるクライアント・サーバ型システムのブロック図である。

【図 3 7】

本発明の第 9 の実施の形態の動作例を示すシーケンスチャートである。

【符号の説明】

- 1 …サーバ装置
- 1 1 …要求受付部
- 1 2 …要求転送部
- 1 3 …暗号化部
- 2 …サーバ装置用のローカル保守コンソール
- 3 …クライアント装置
- 3 1 …保守対象部
- 3 2 …利用者認証部
- 3 3 …リモート要求処理部
- 3 4 …ローカル要求処理部
- 3 5 …ログイン・ログアウト処理部
- 3 6 …復号化部
- 3 7 …強制切断部
- 3 8 …利用時間管理部
- 3 9 …ログイン回数管理部
- 3 A - 1 …利用可能時間基準値

3 A - 2 ... ログイン可能回数基準値

3 B ... 利用時間延長部

3 C ... 認証無効化部

4 ... クライアント装置用のローカル保守コンソール

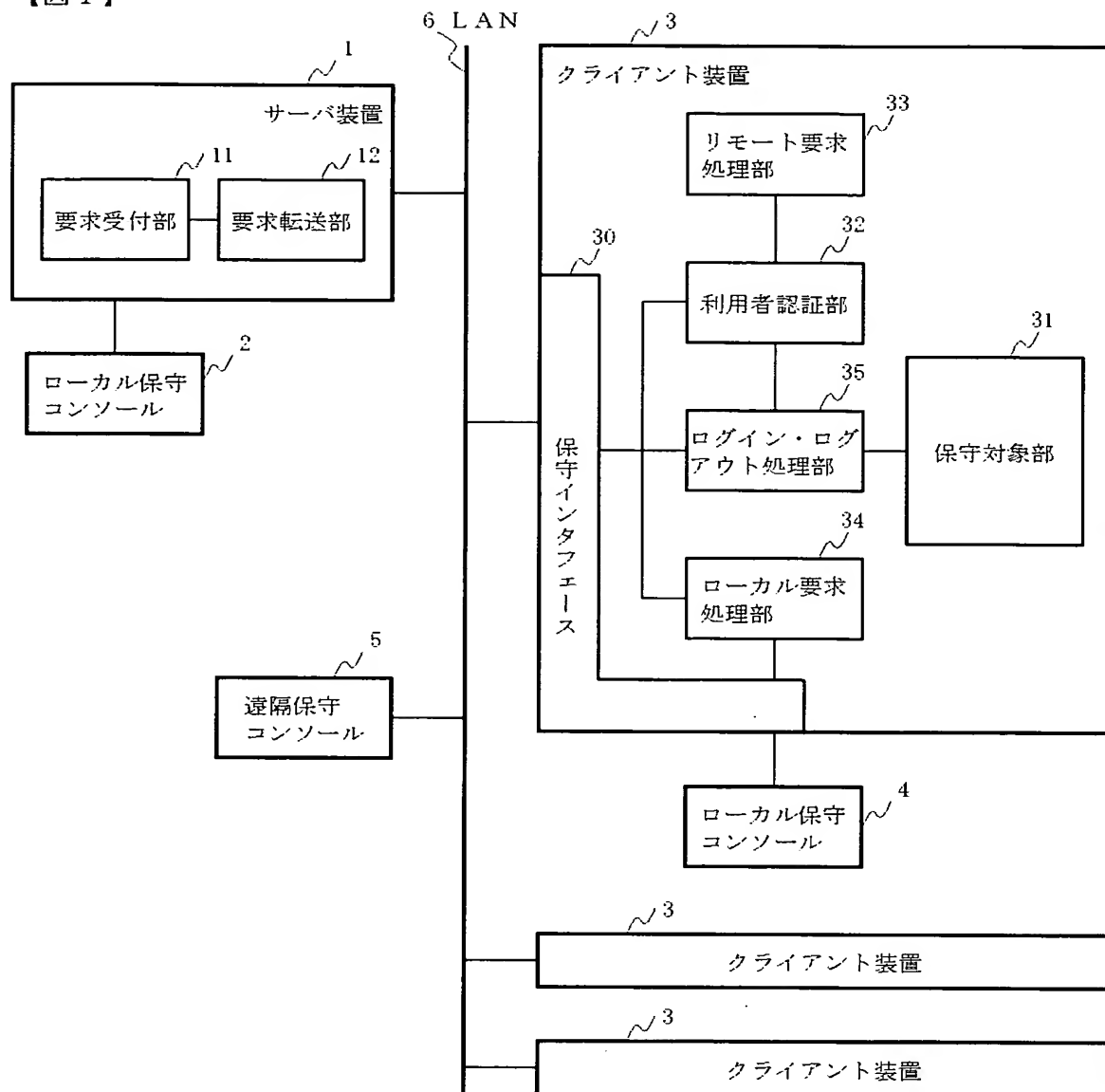
5 ... 遠隔保守コンソール

6 ... L A N

【書類名】 図面

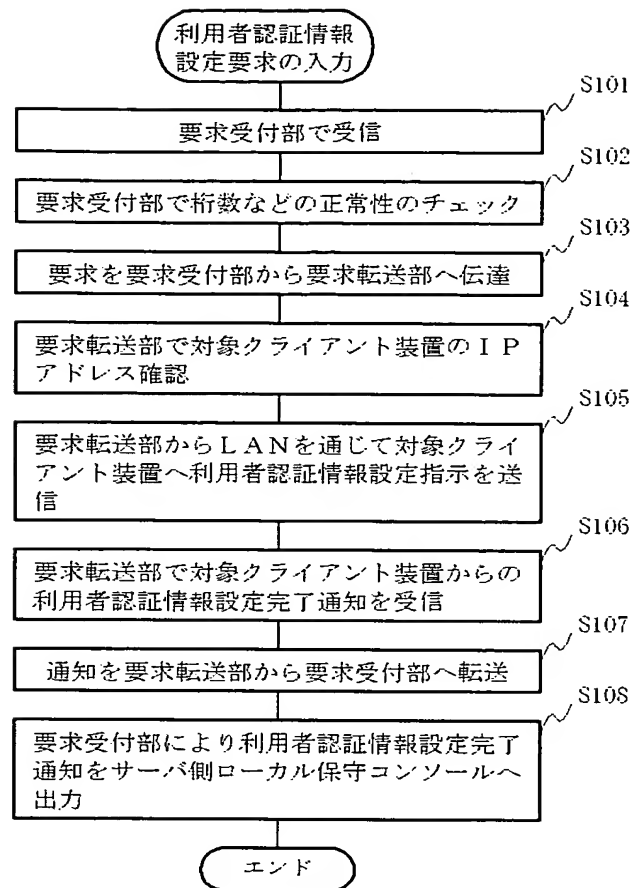
【図 1】

【図 1】



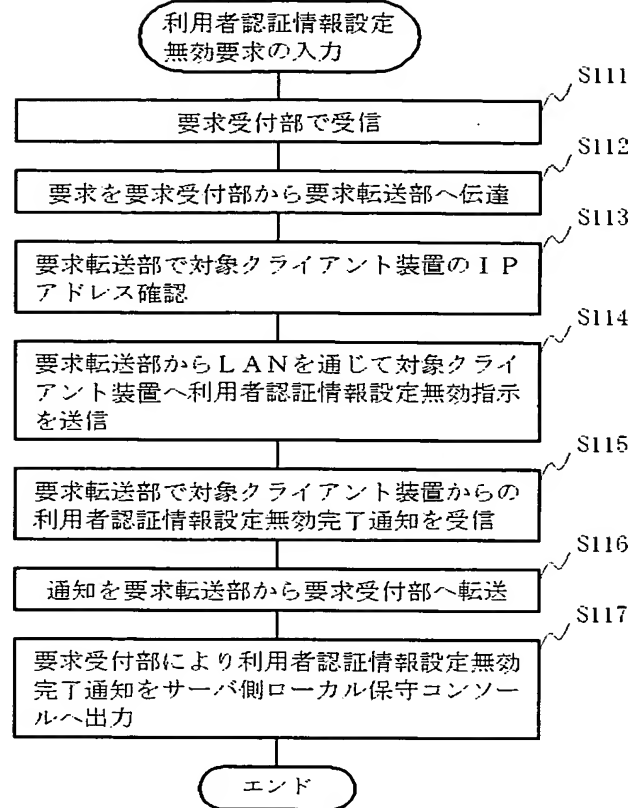
【図 2】

【図 2】



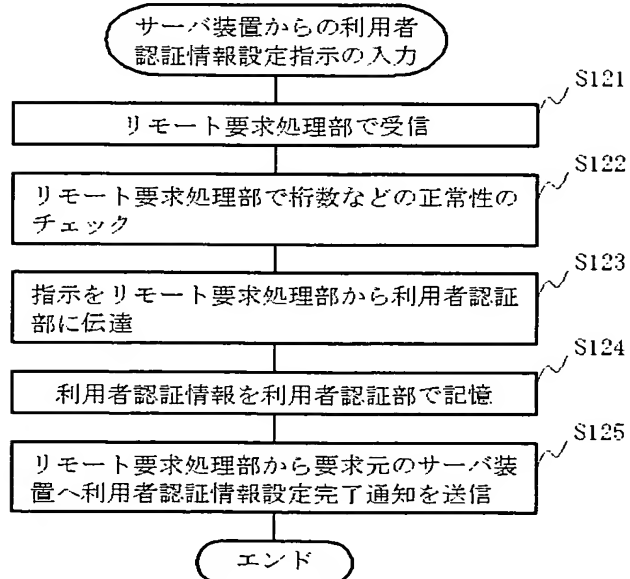
【図 3】

【図 3】



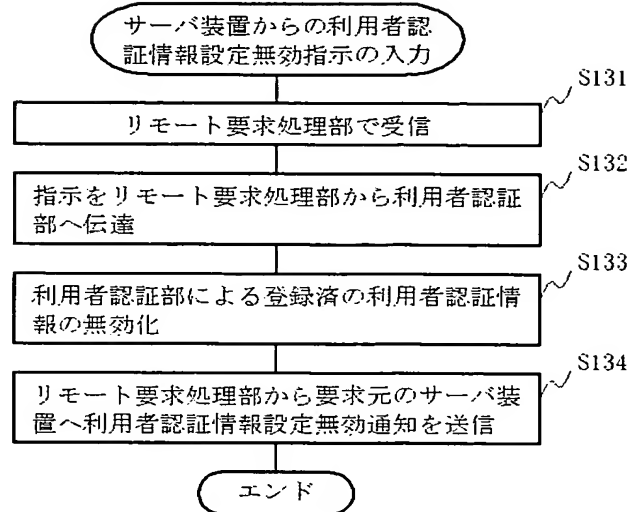
【図 4】

【図 4】



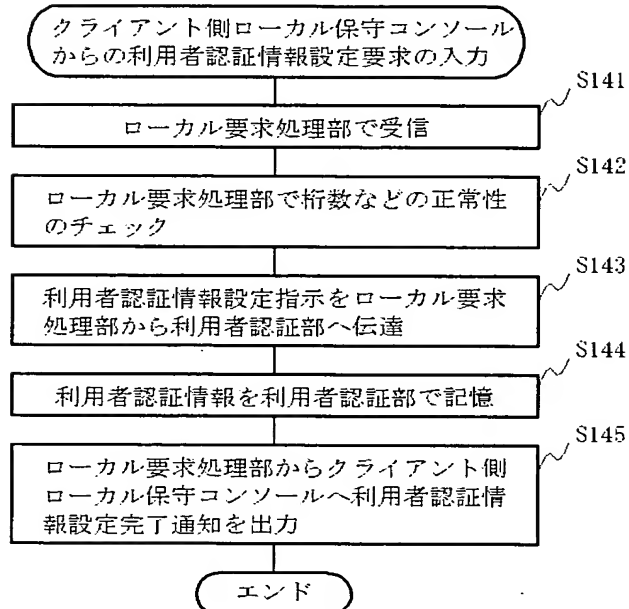
【図 5】

【図 5】



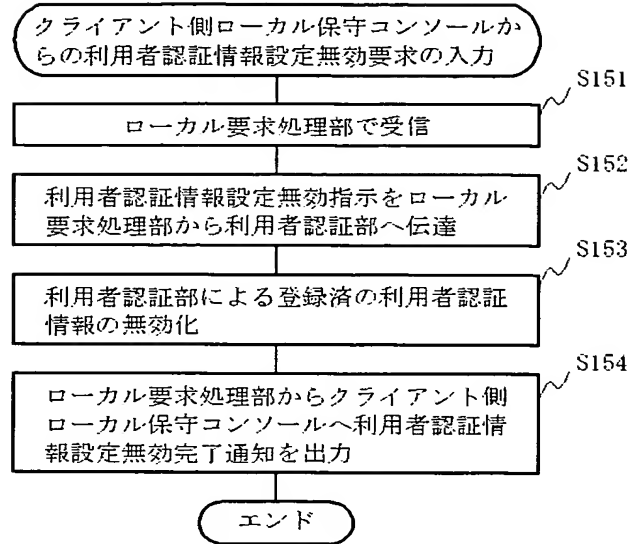
【図 6】

【図 6】



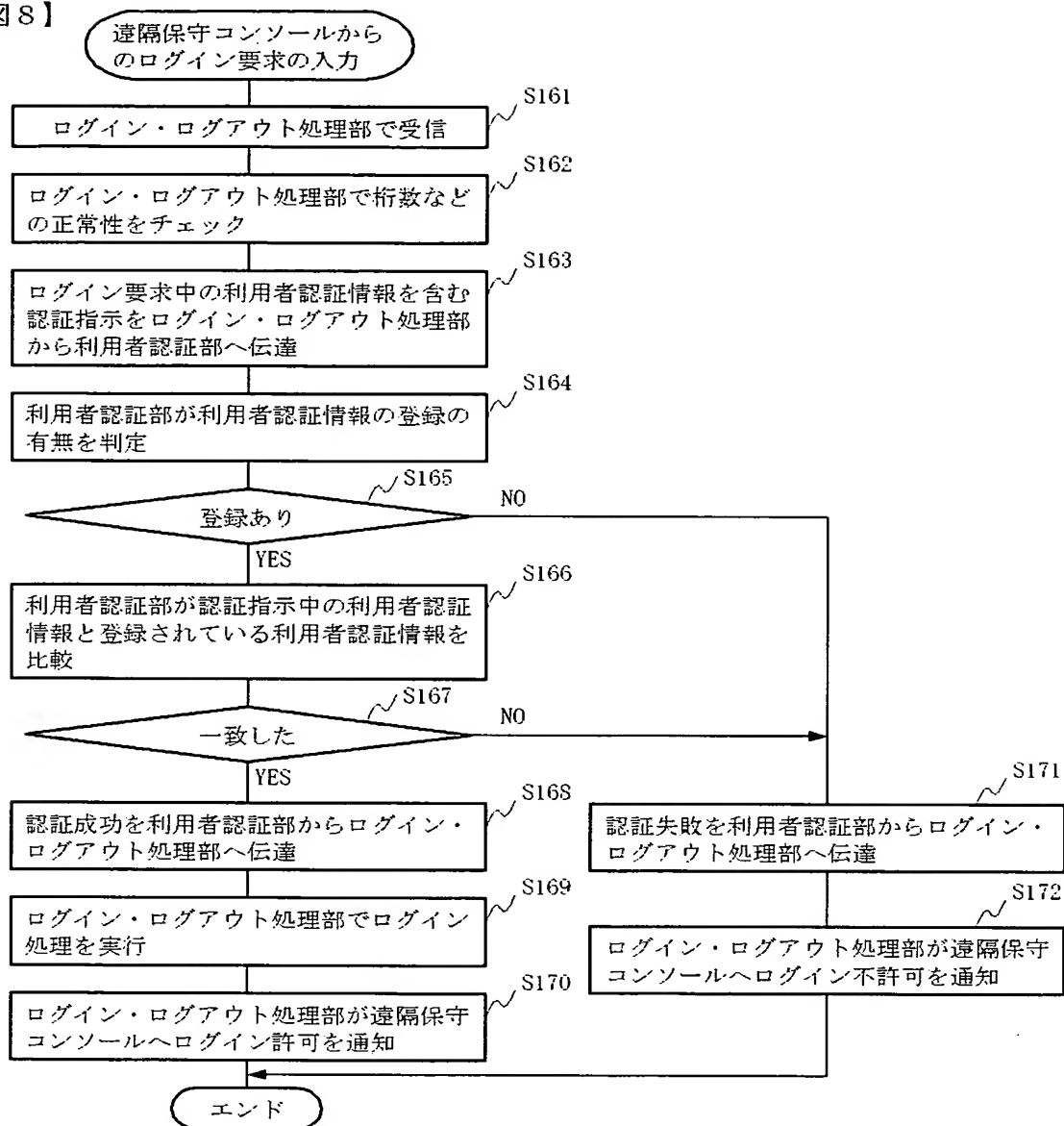
【図 7】

【図 7】



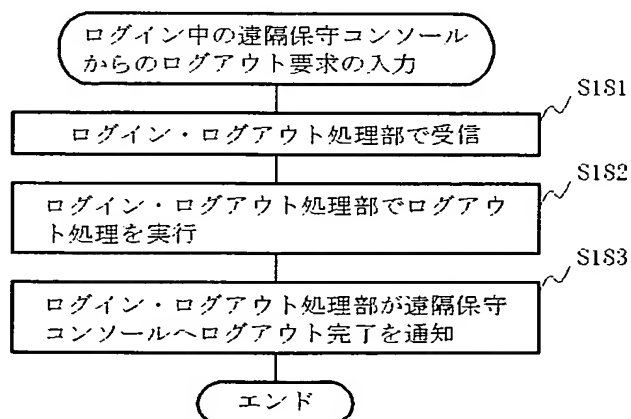
【図 8】

【図 8】



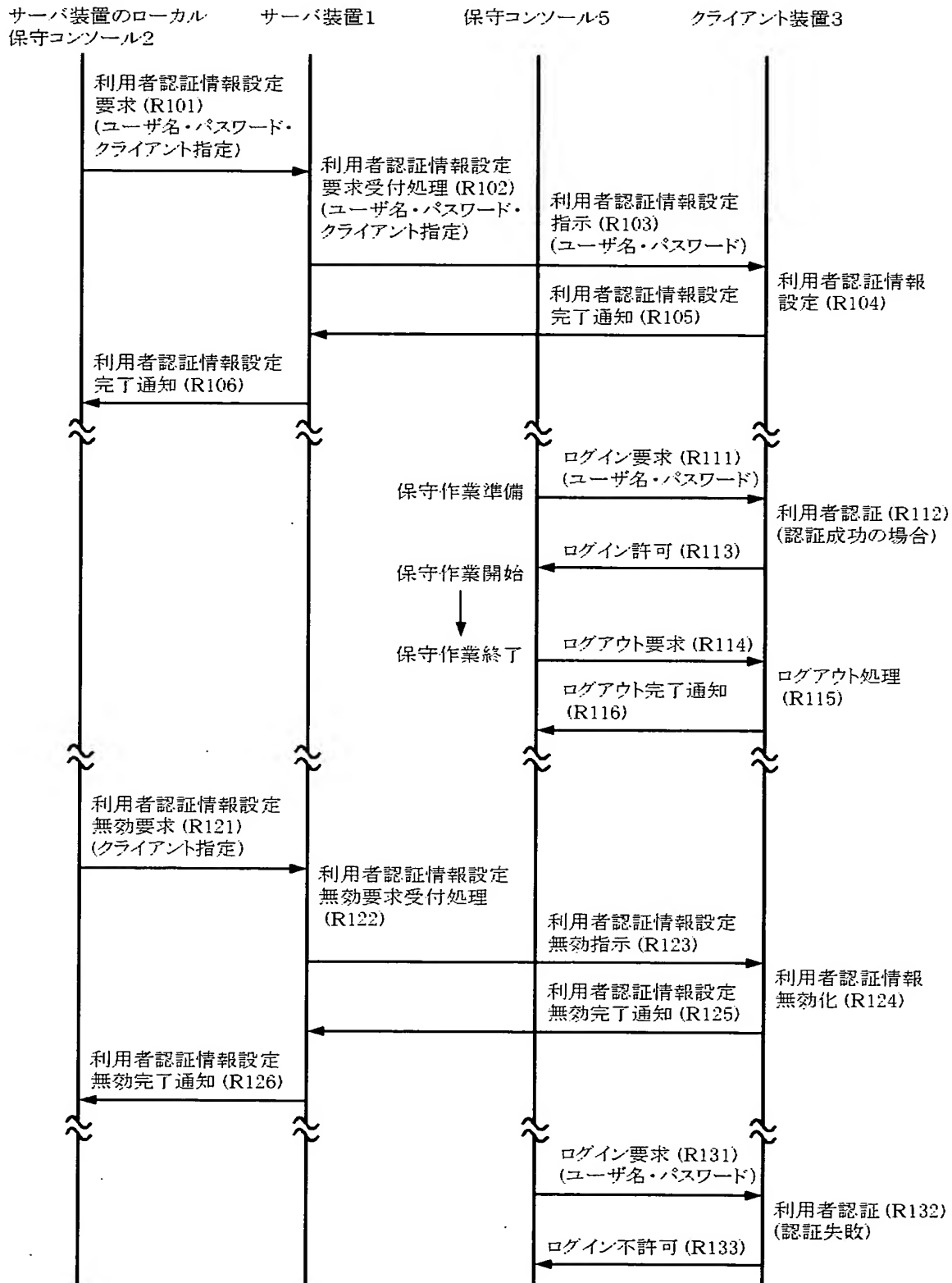
【図 9】

【図 9】



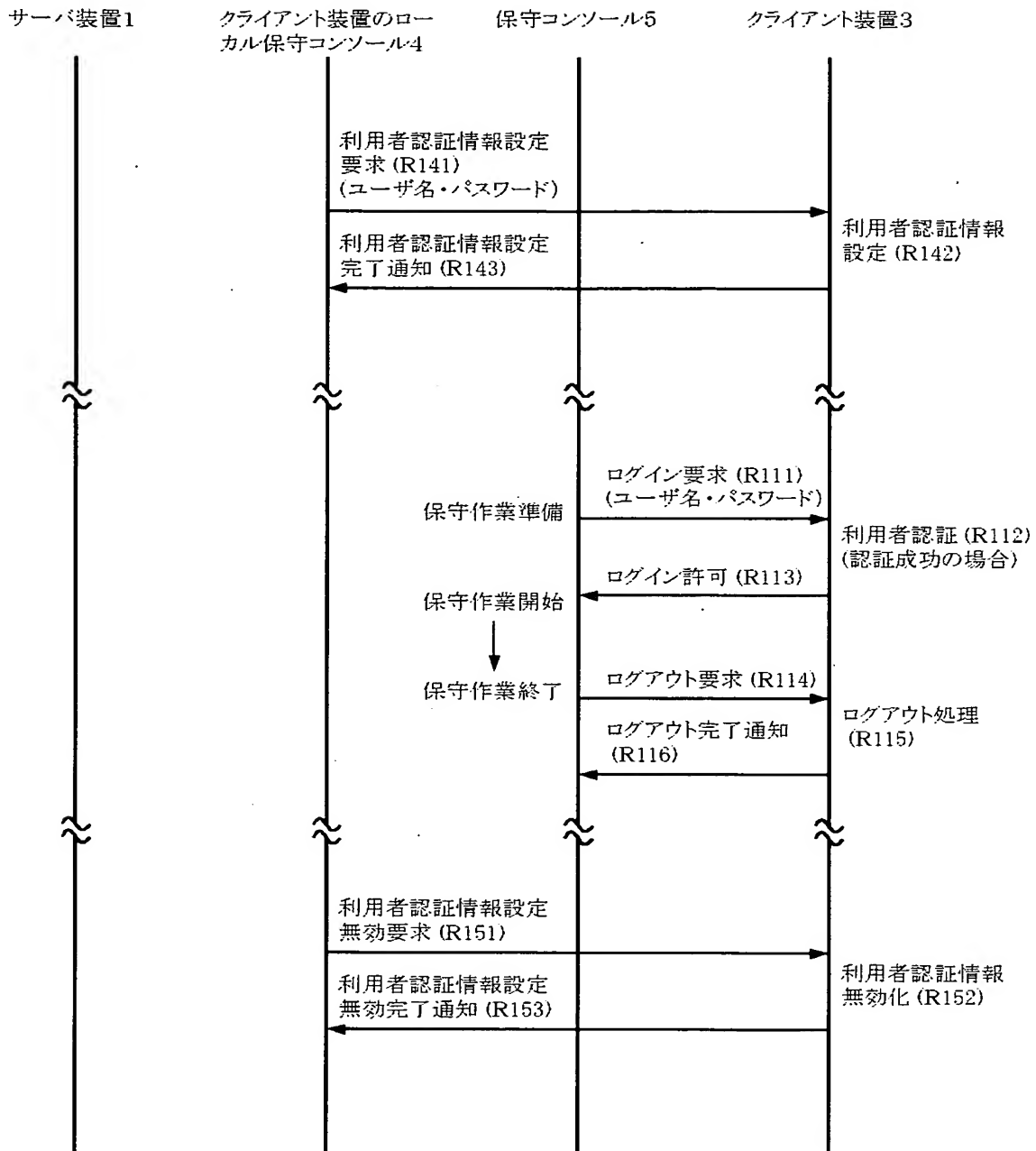
【図 10】

【図 10】



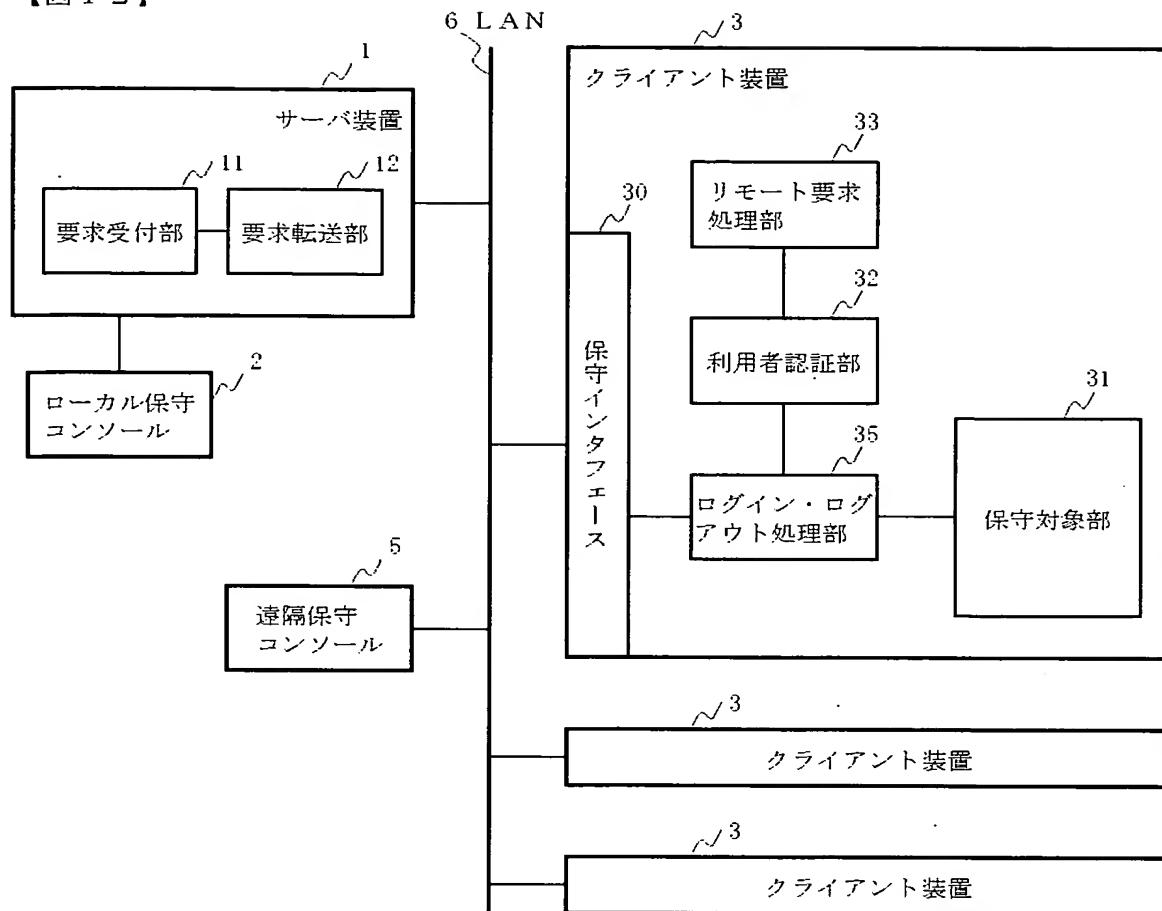
【図 11】

【図 11】



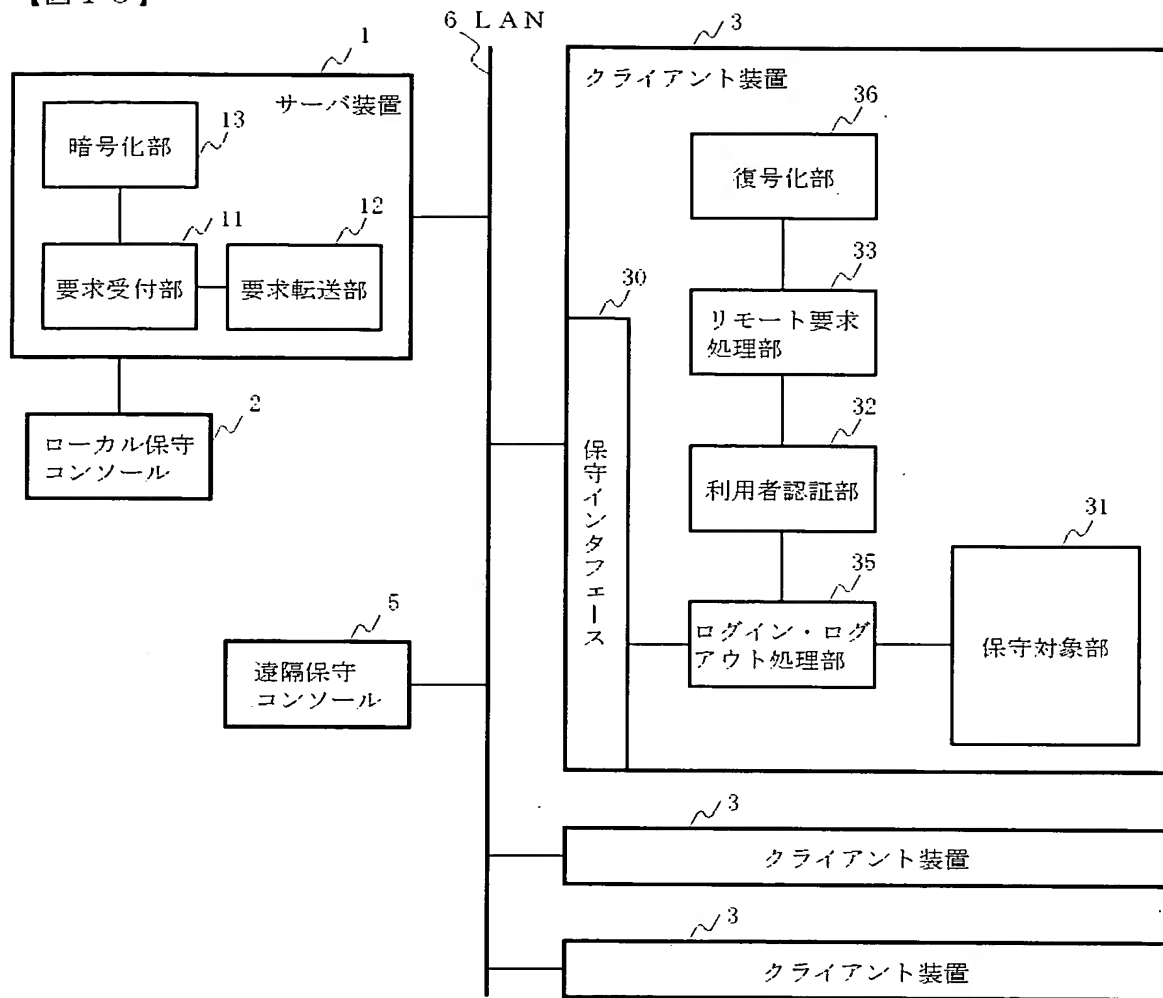
【図 12】

【図 12】



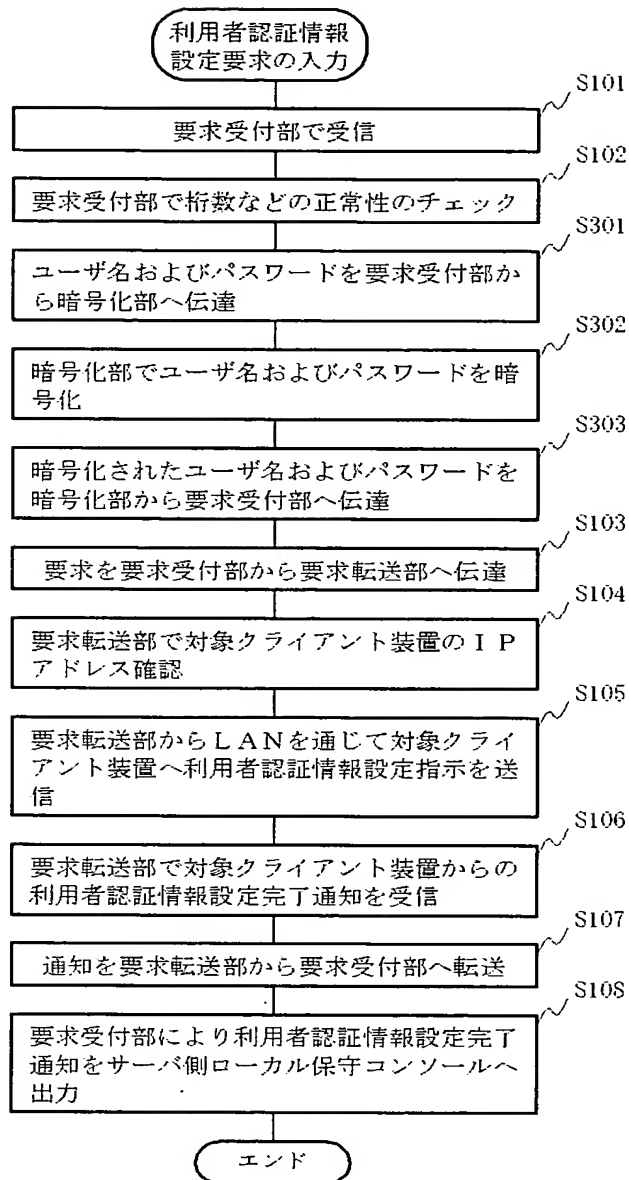
【図 13】

【図 13】



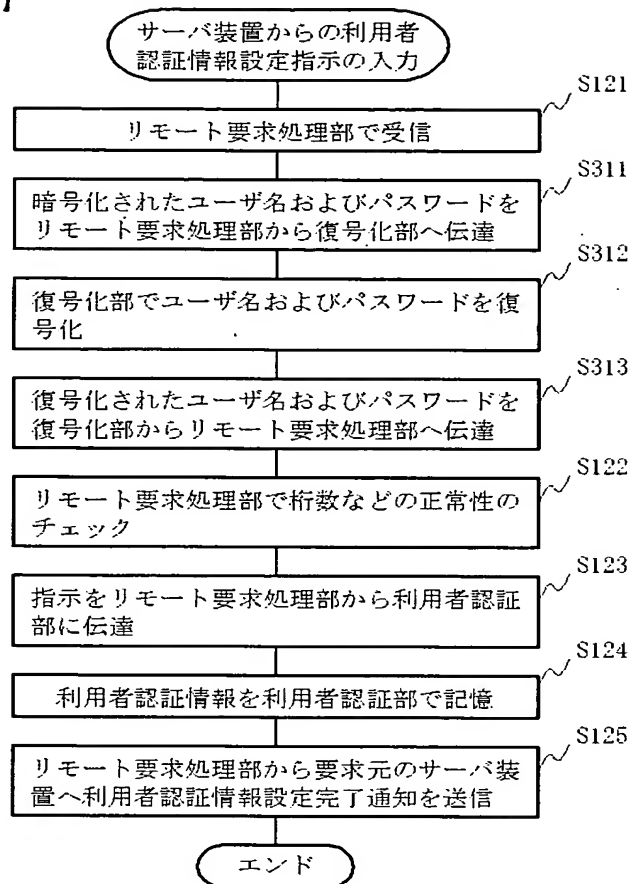
【図 14】

【図 14】



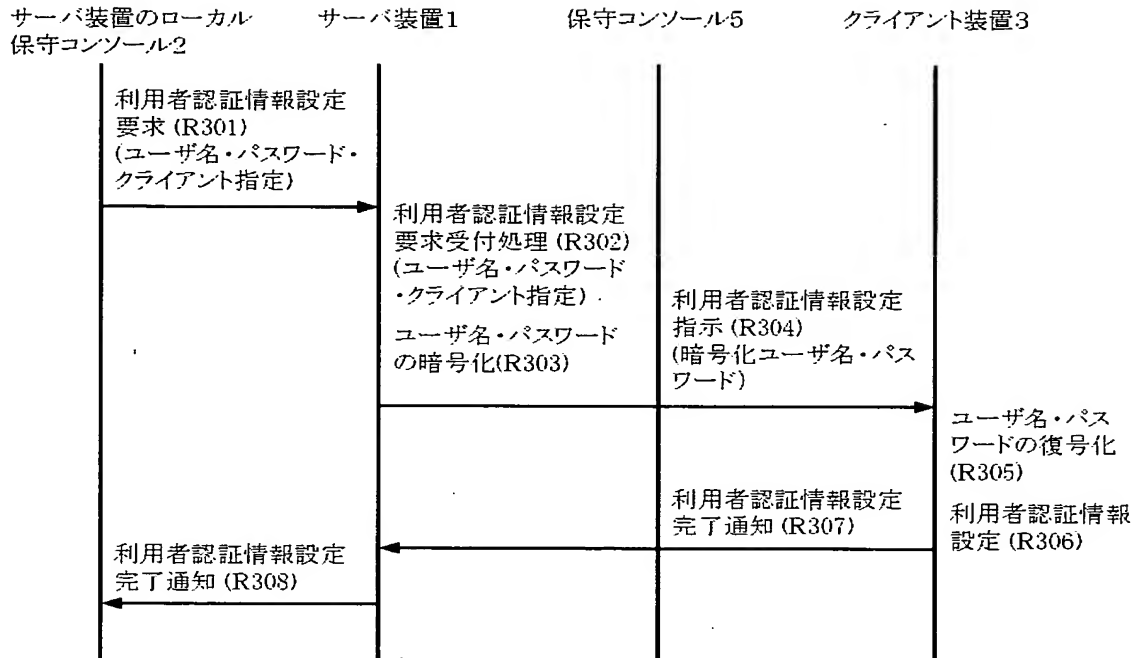
【図 15】

【図 15】



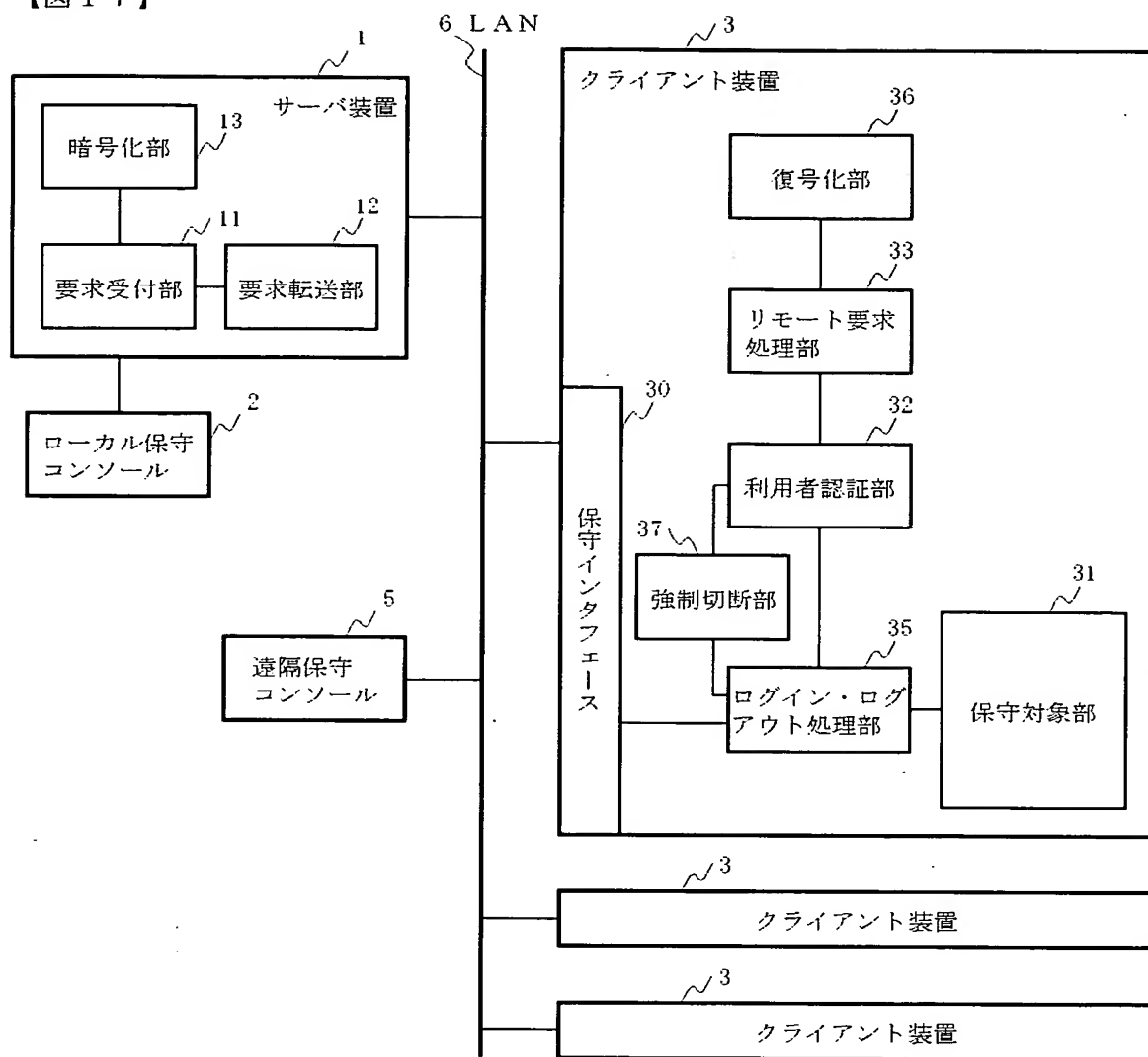
【図 16】

【図 16】



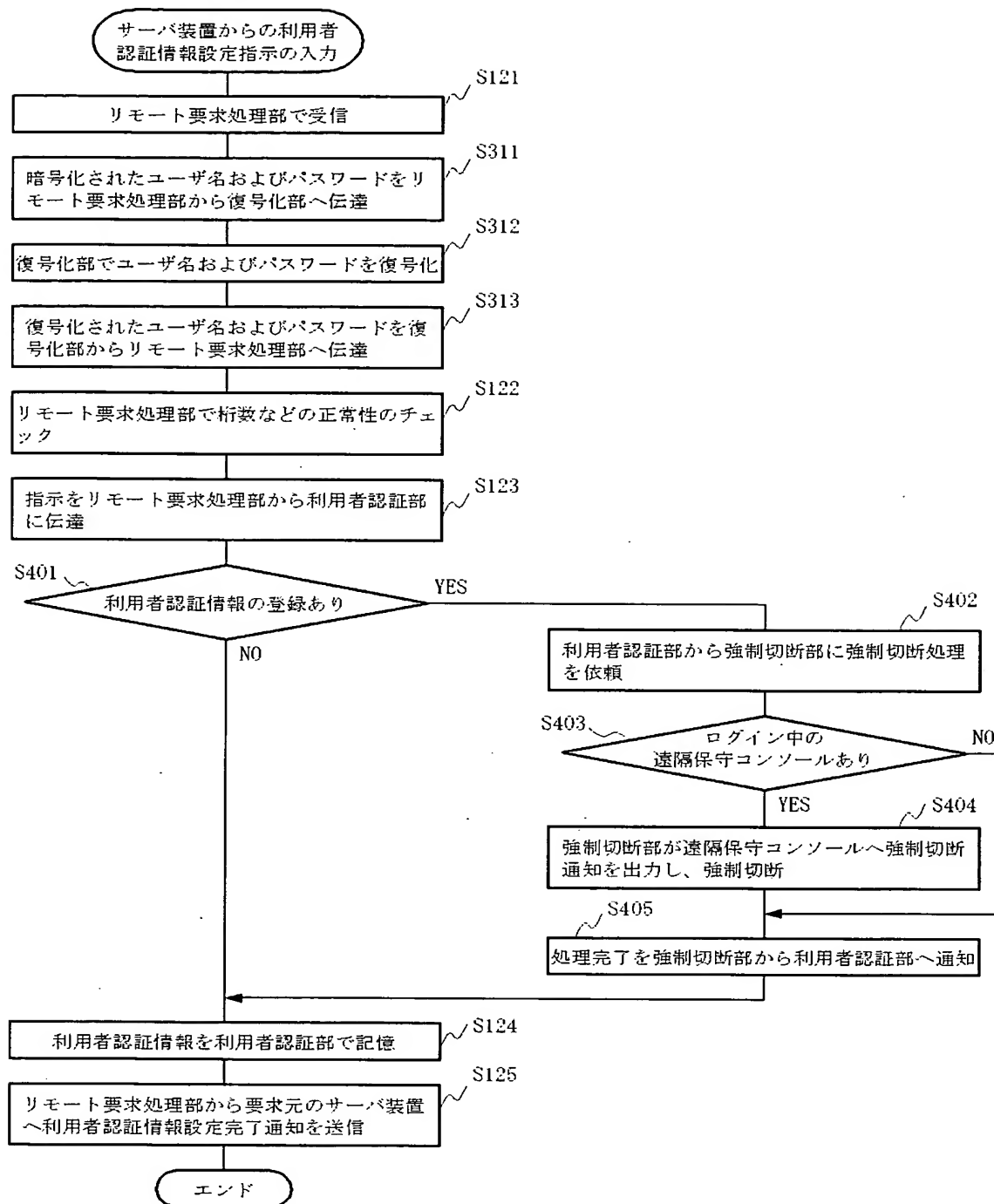
【図 17】

【図 17】



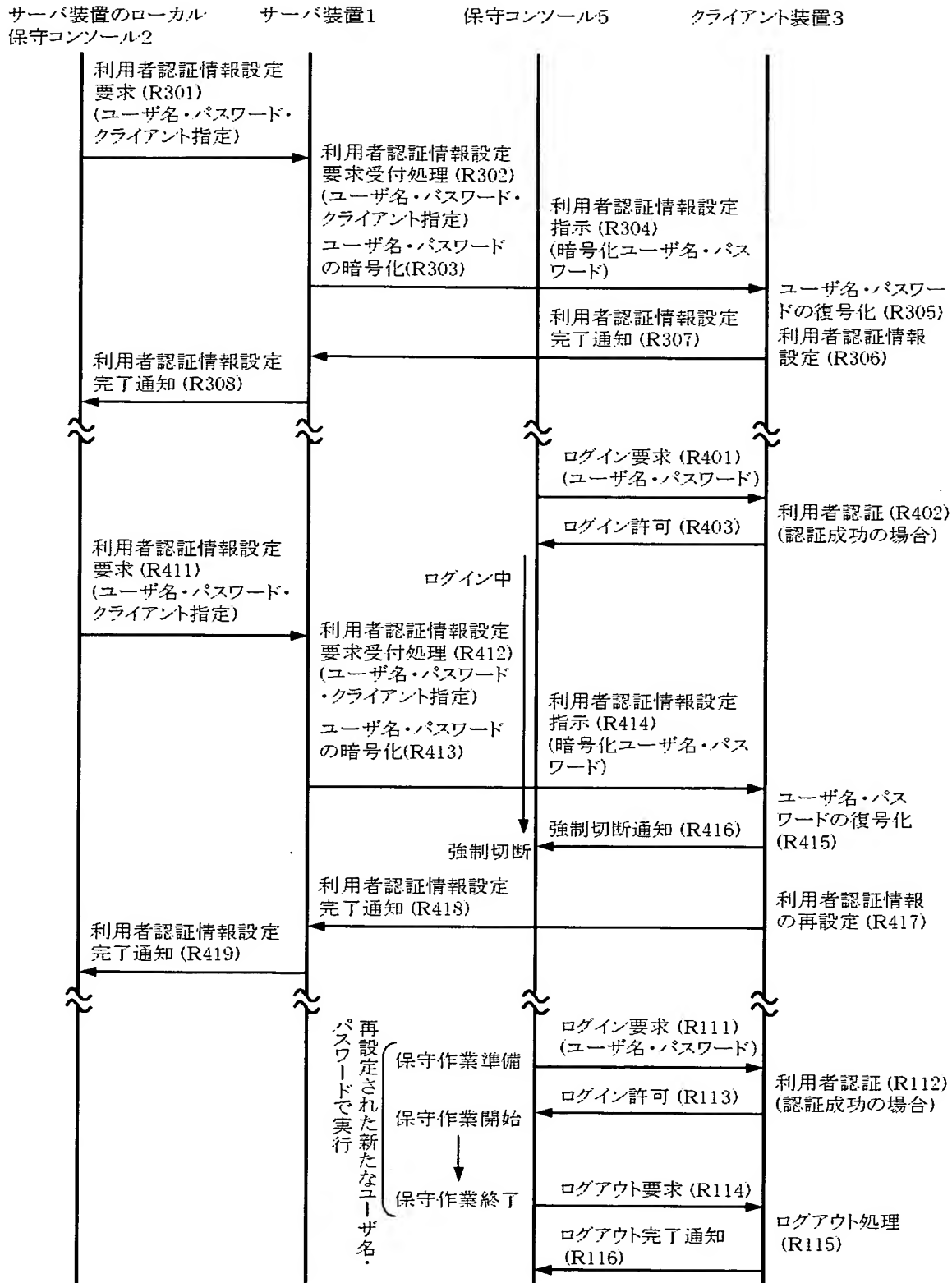
【図 18】

【図 18】



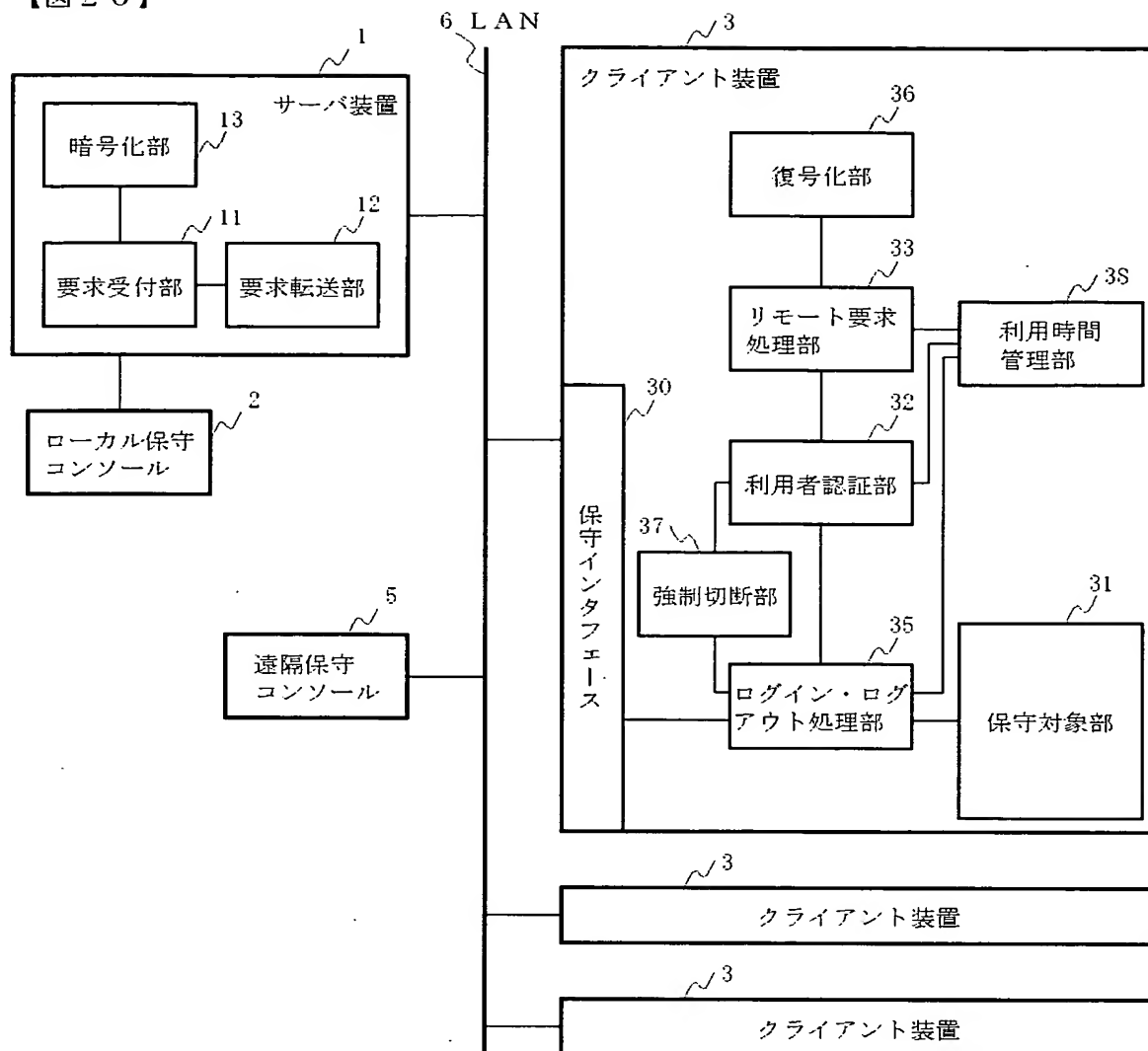
【図 19】

【図 19】



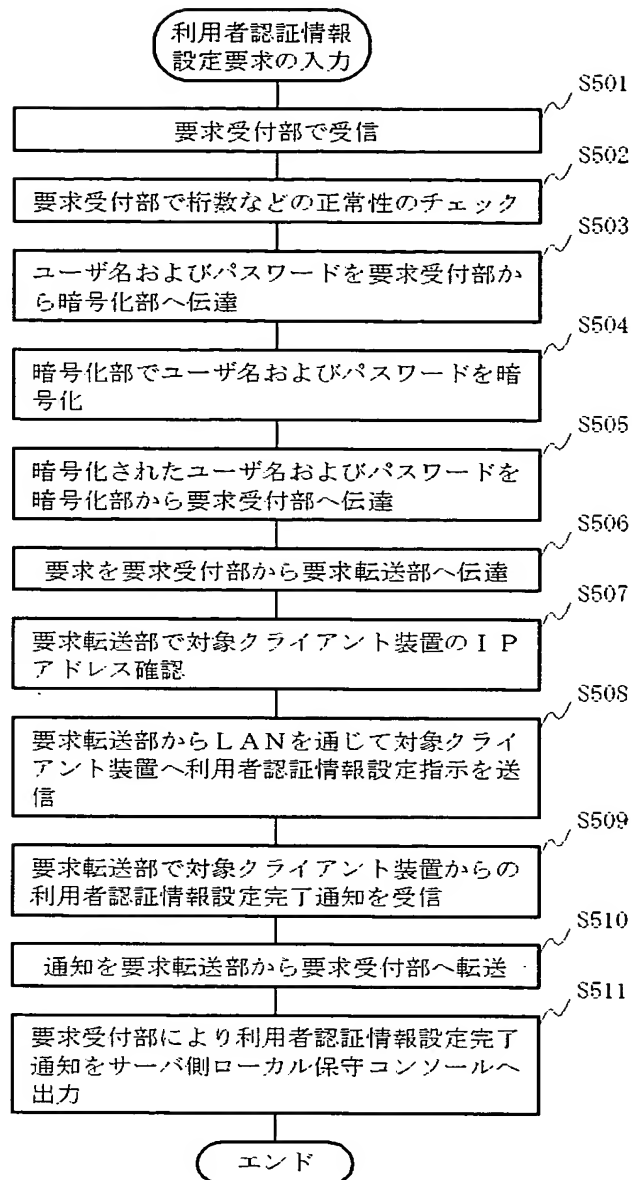
【図 20】

【図 20】



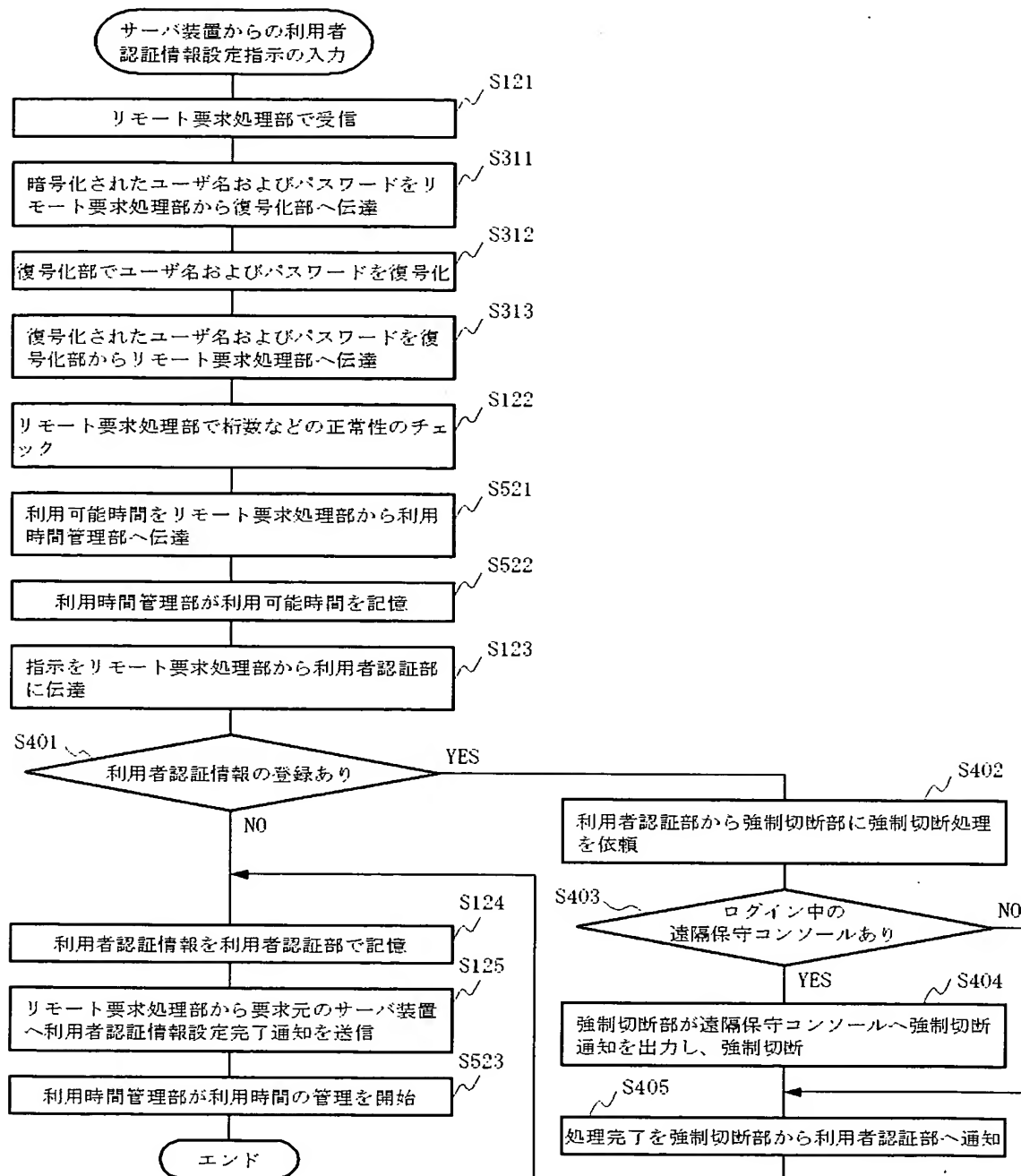
【図 21】

【図 21】



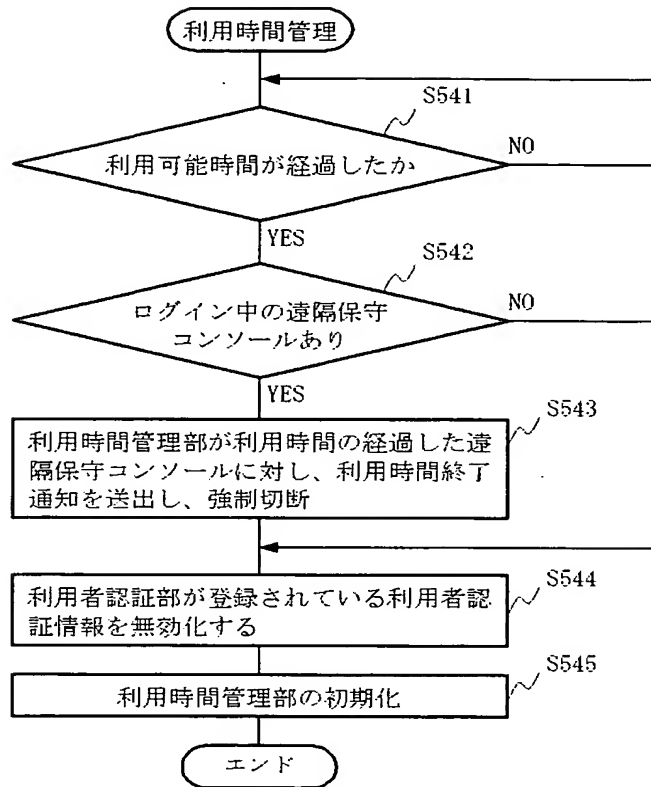
【図 22】

【図 22】



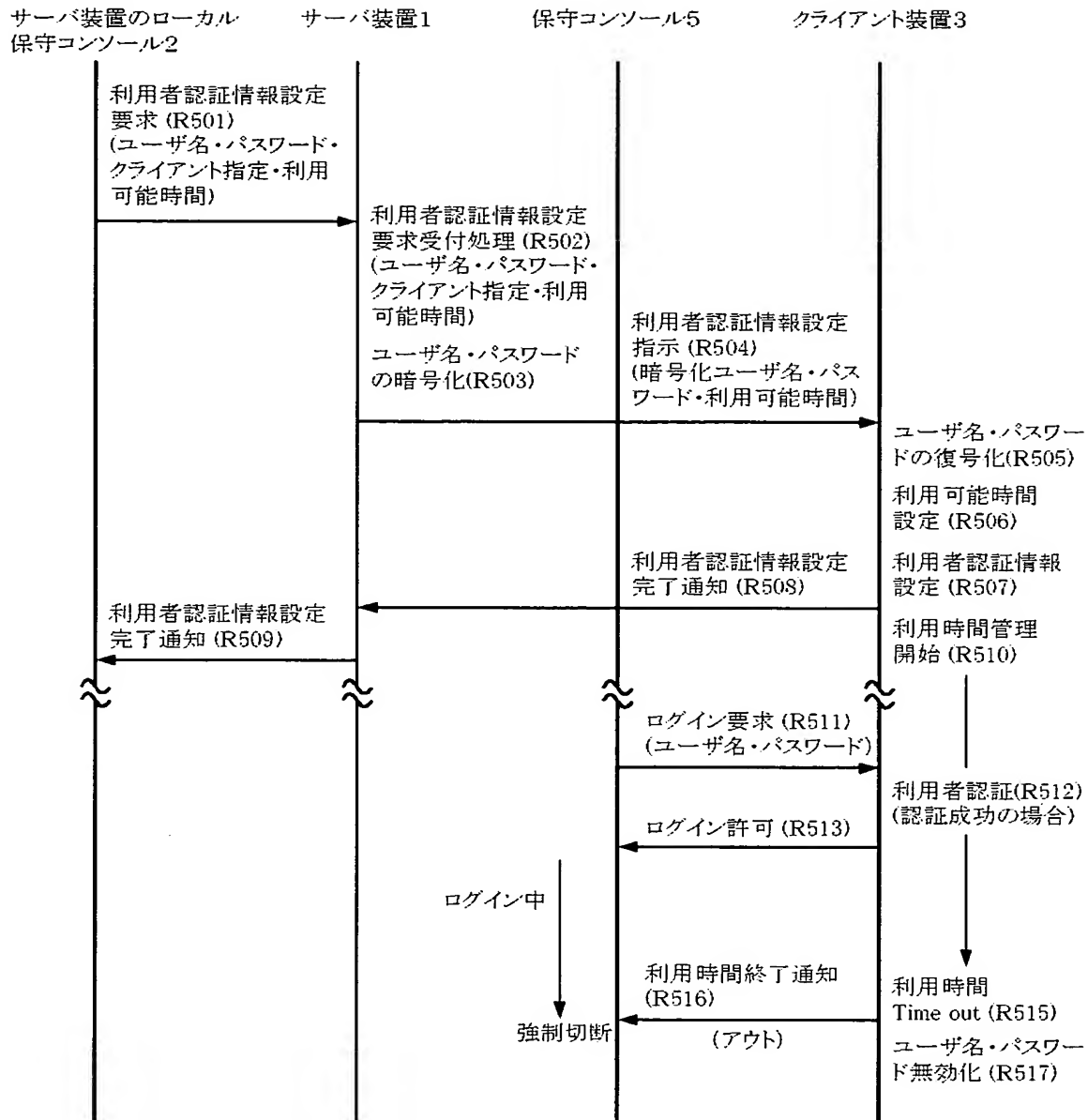
【図 23】

【図 23】



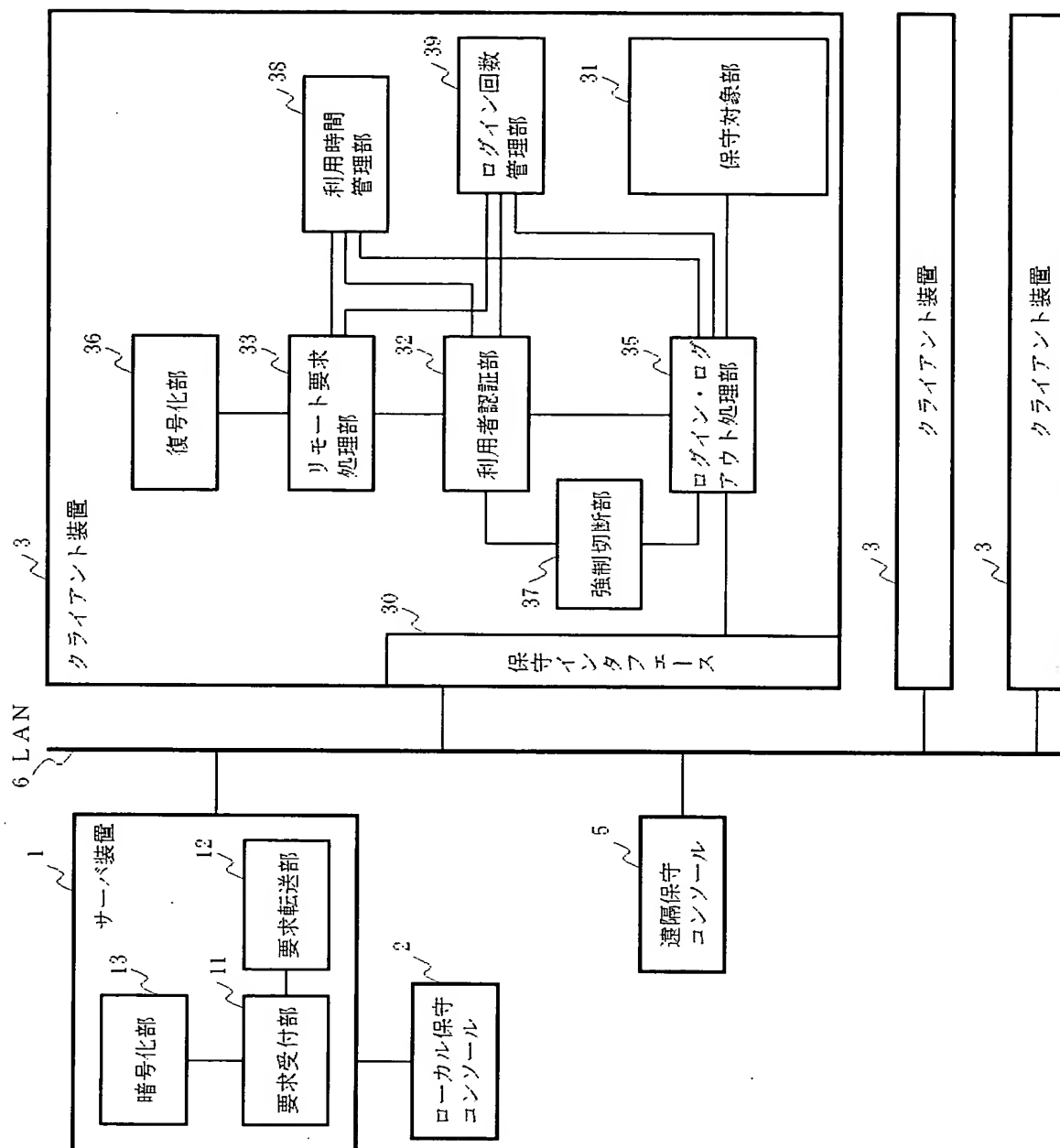
【図 24】

【図 24】



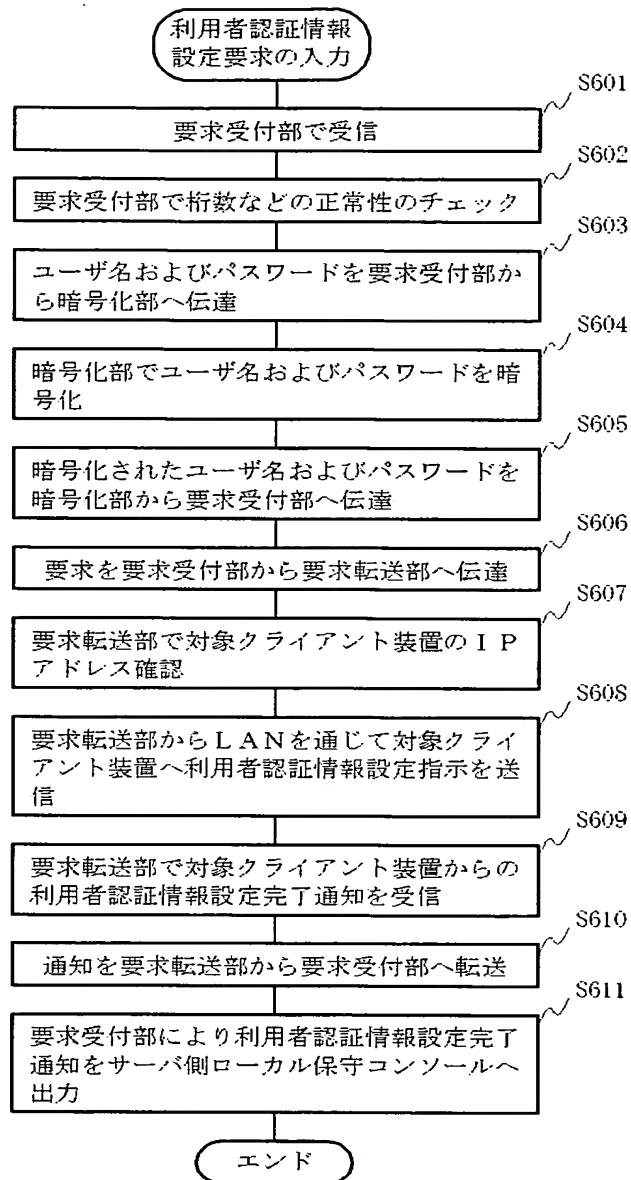
【図 25】

【図 25】



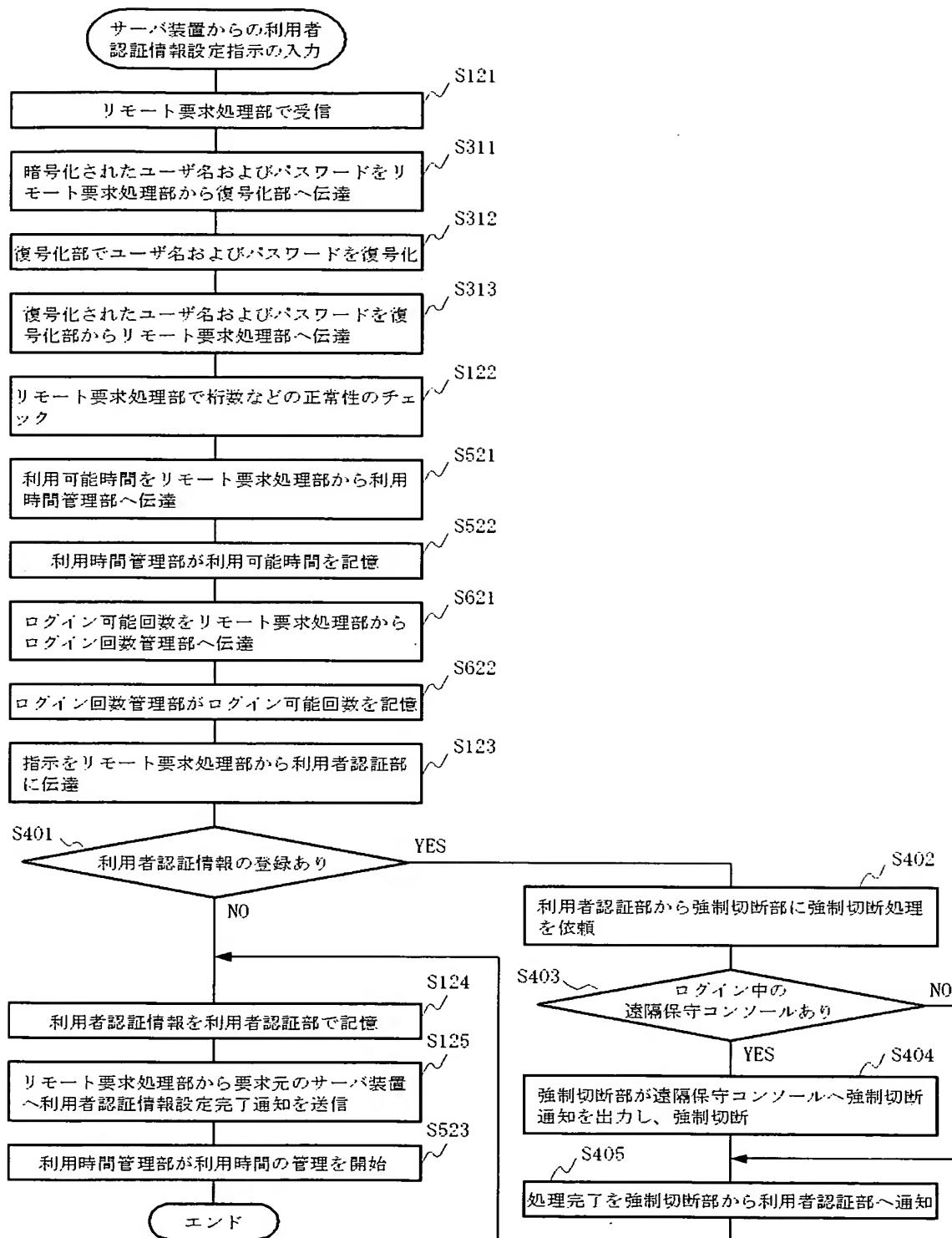
【図 26】

【図 26】



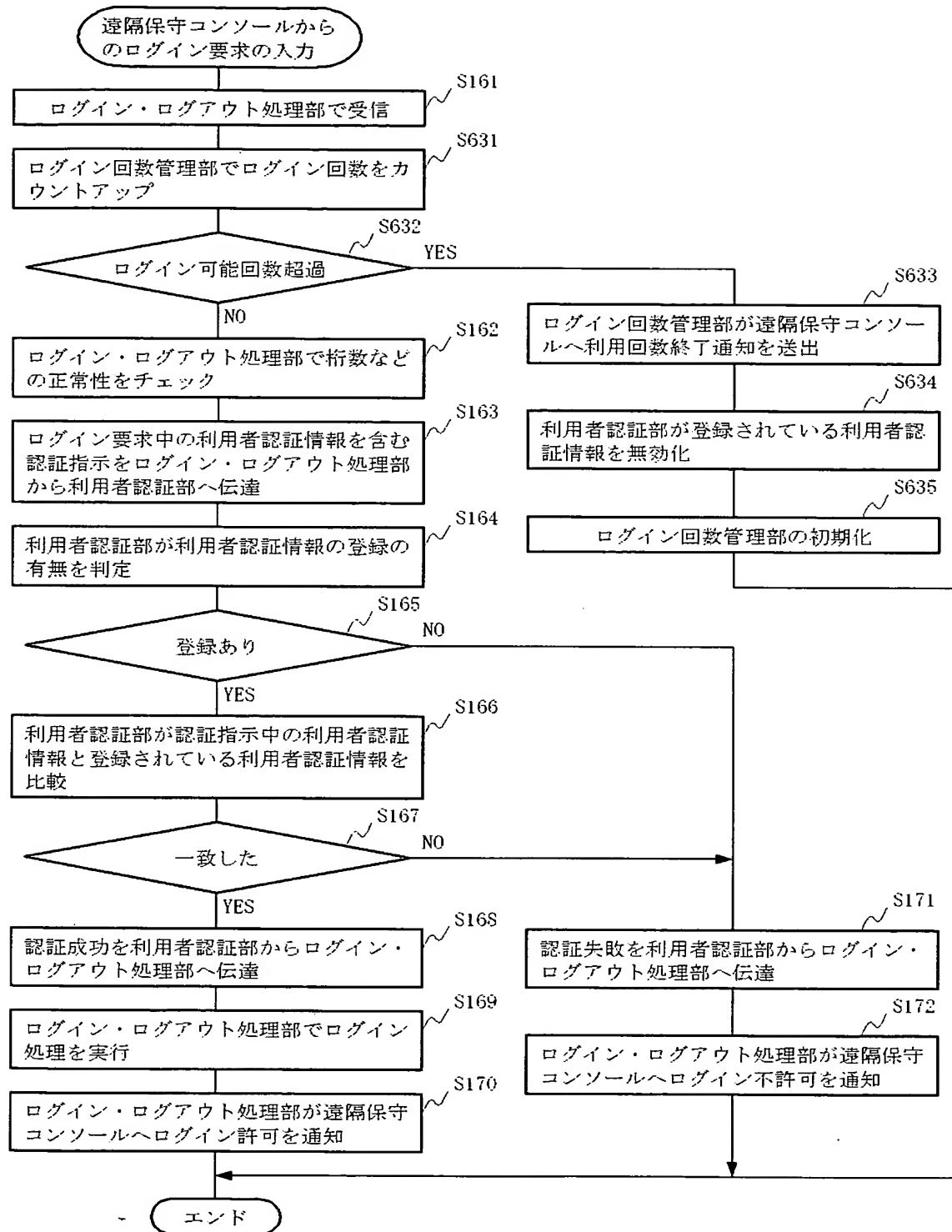
【図 27】

【図 27】



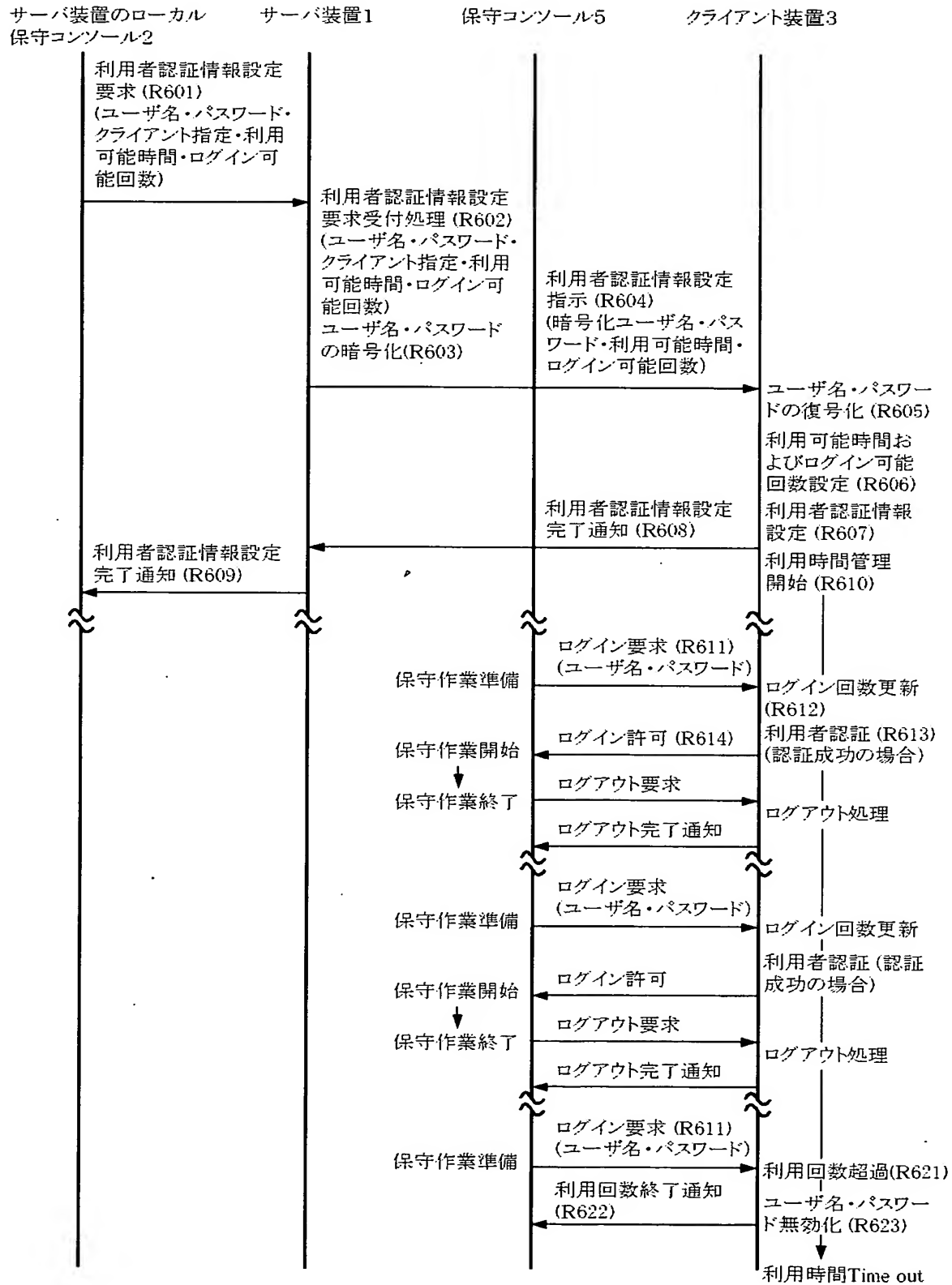
【図 28】

【図 28】



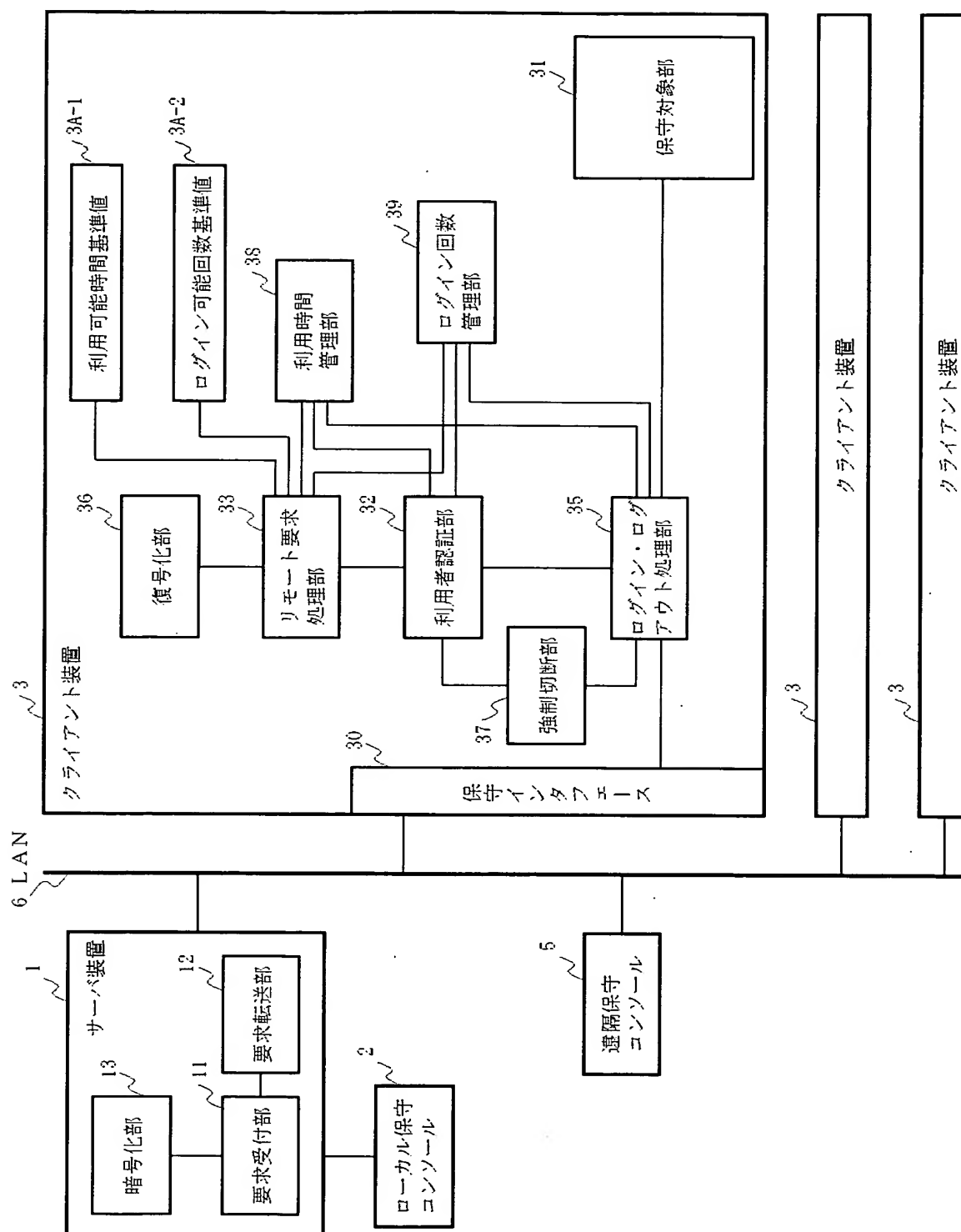
【図 29】

【図 29】



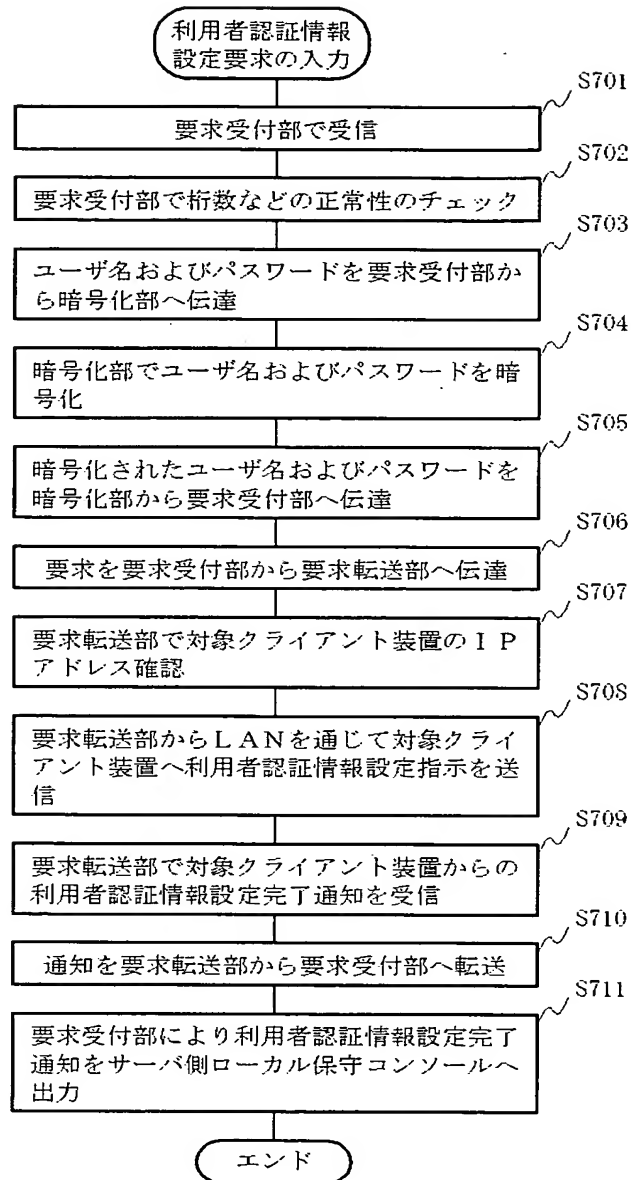
【図 30】

【図 30】



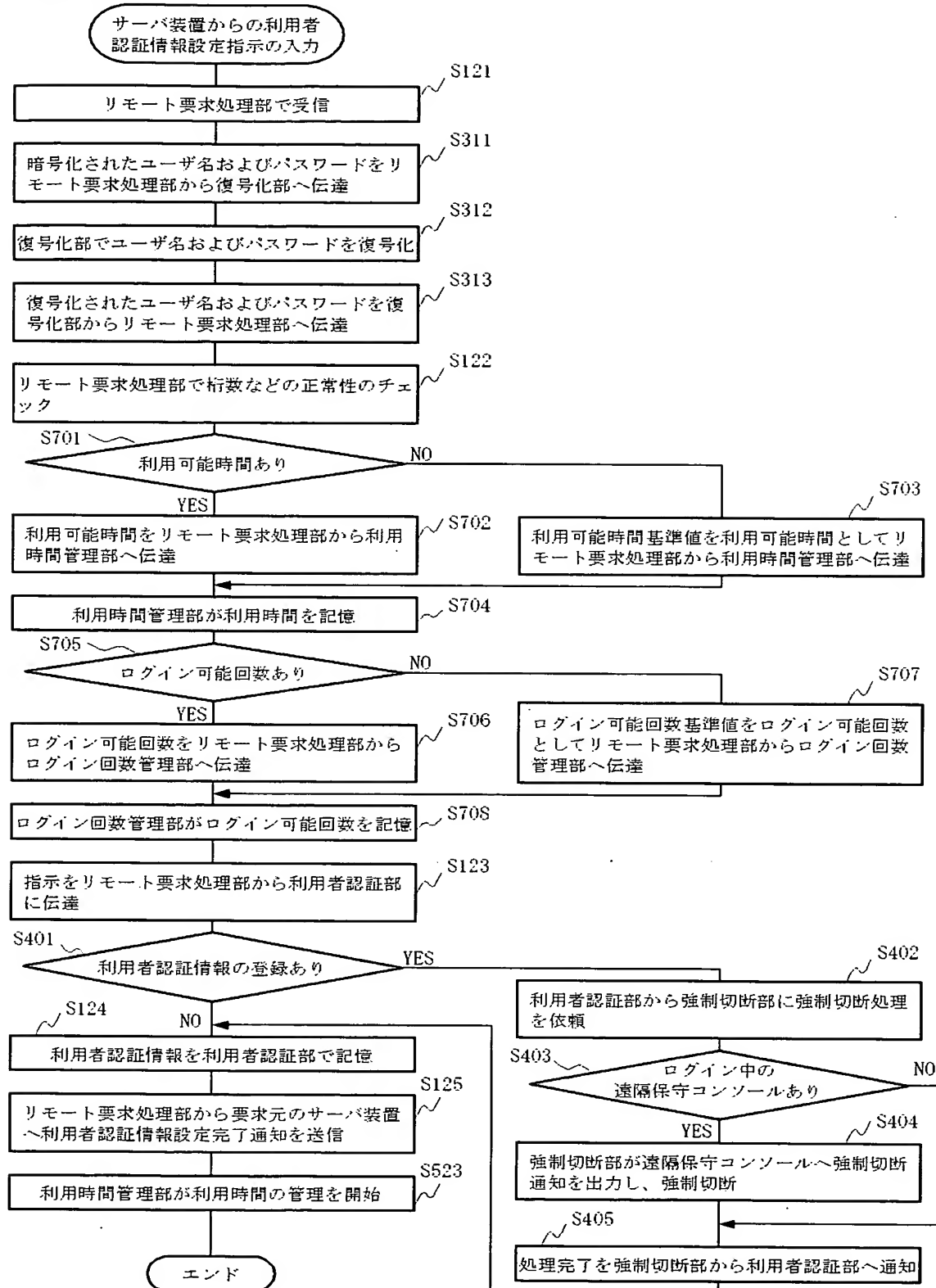
【図 31】

【図 31】



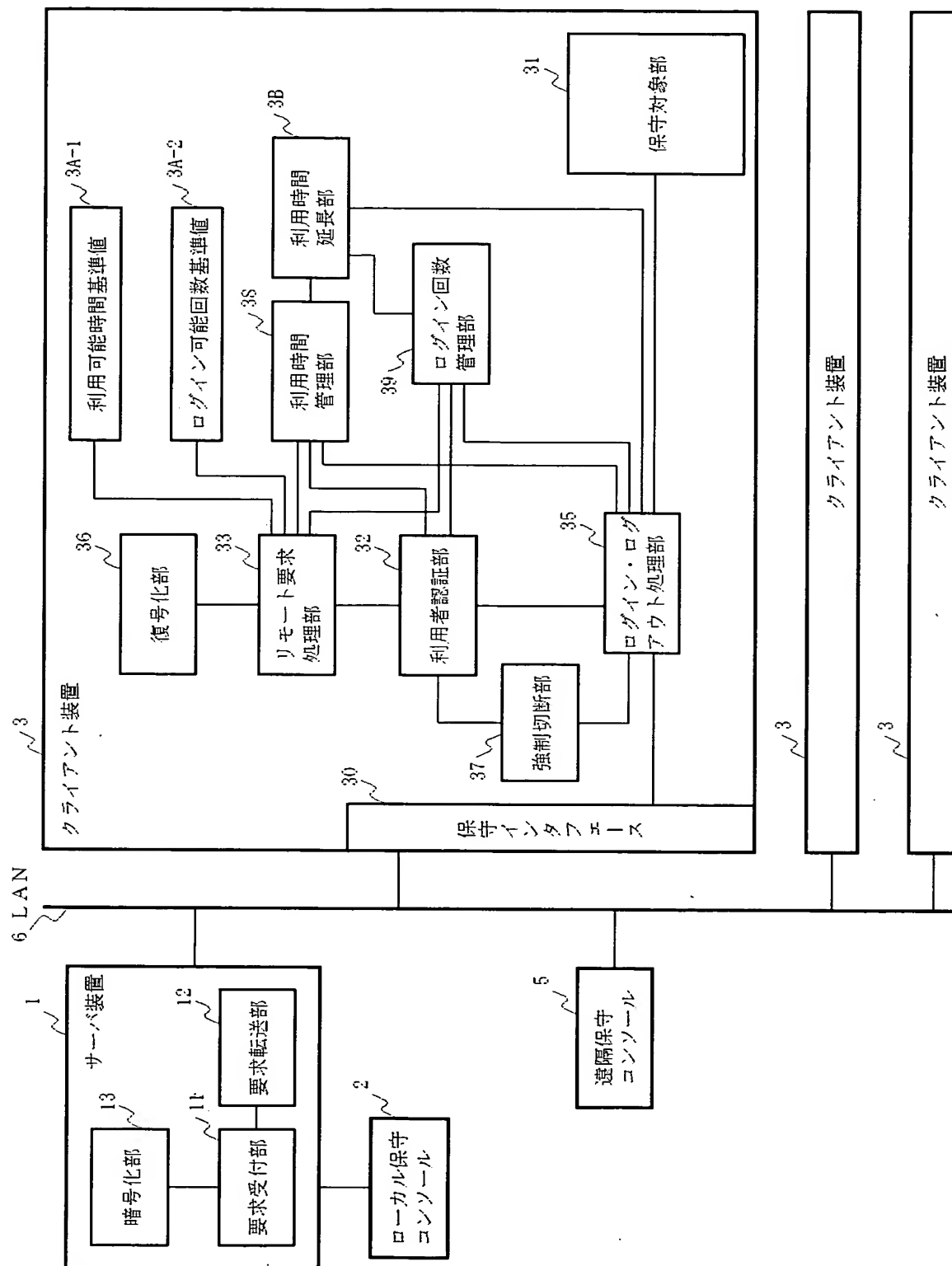
【図 3 2】

【図 3 2】



【図 33】

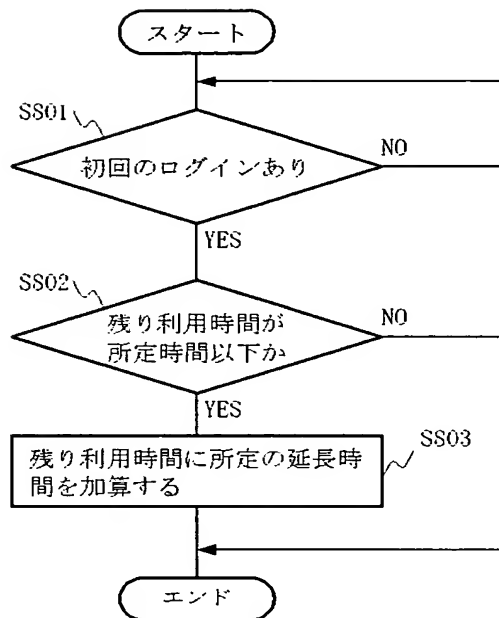
【図 33】



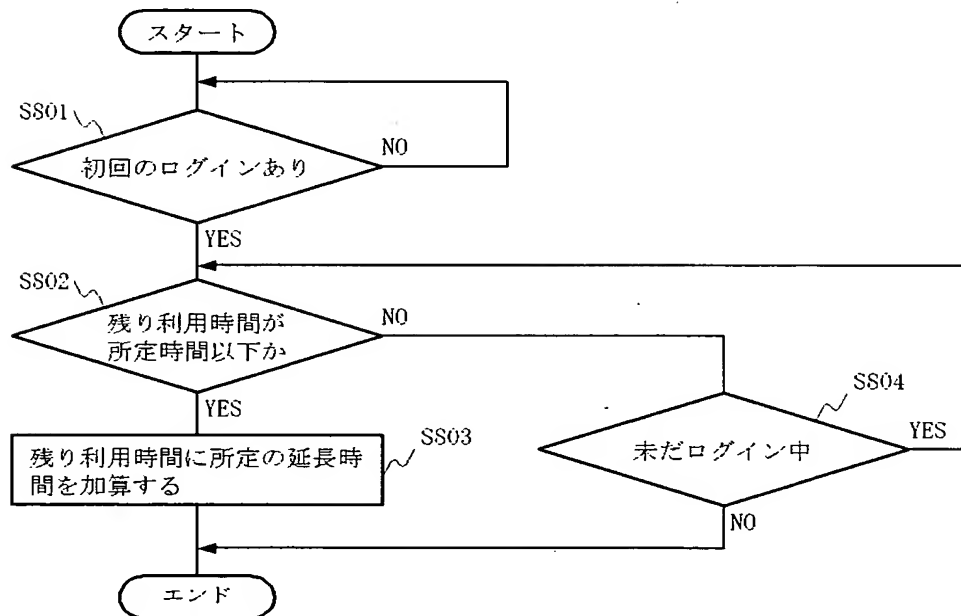
【図 3 4】

【図 3 4】

(A)

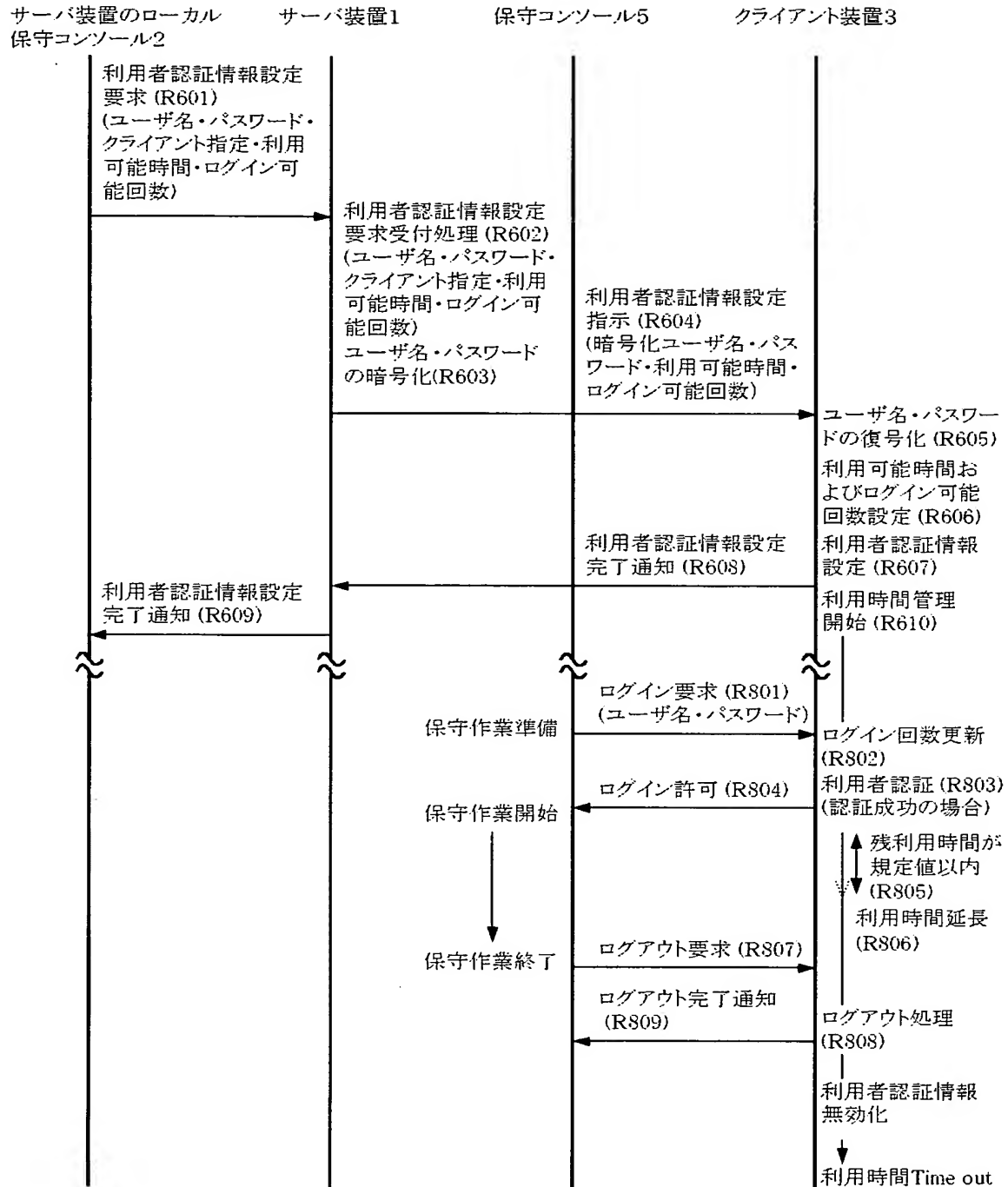


(B)



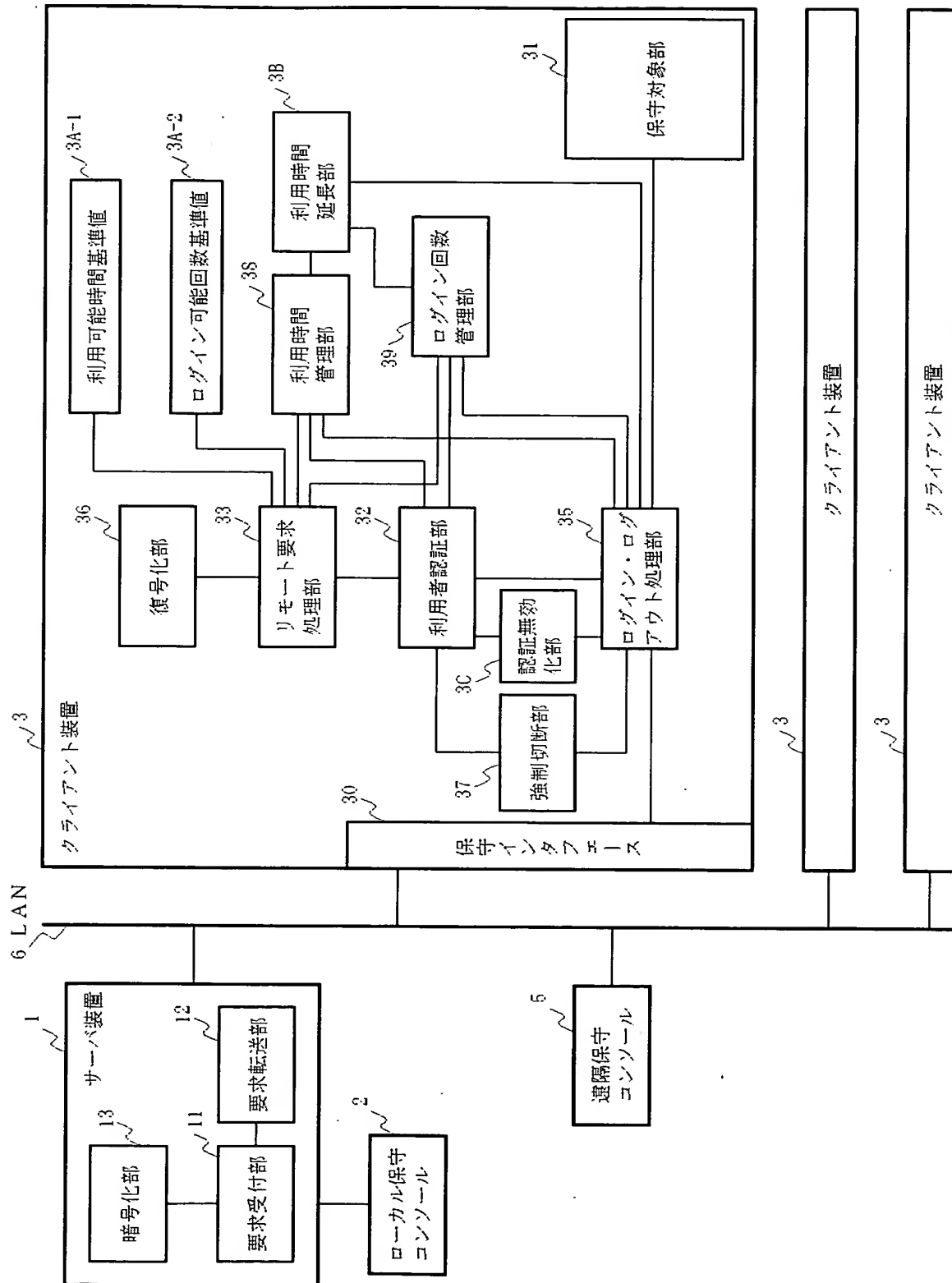
【図 3 5】

【図 35】



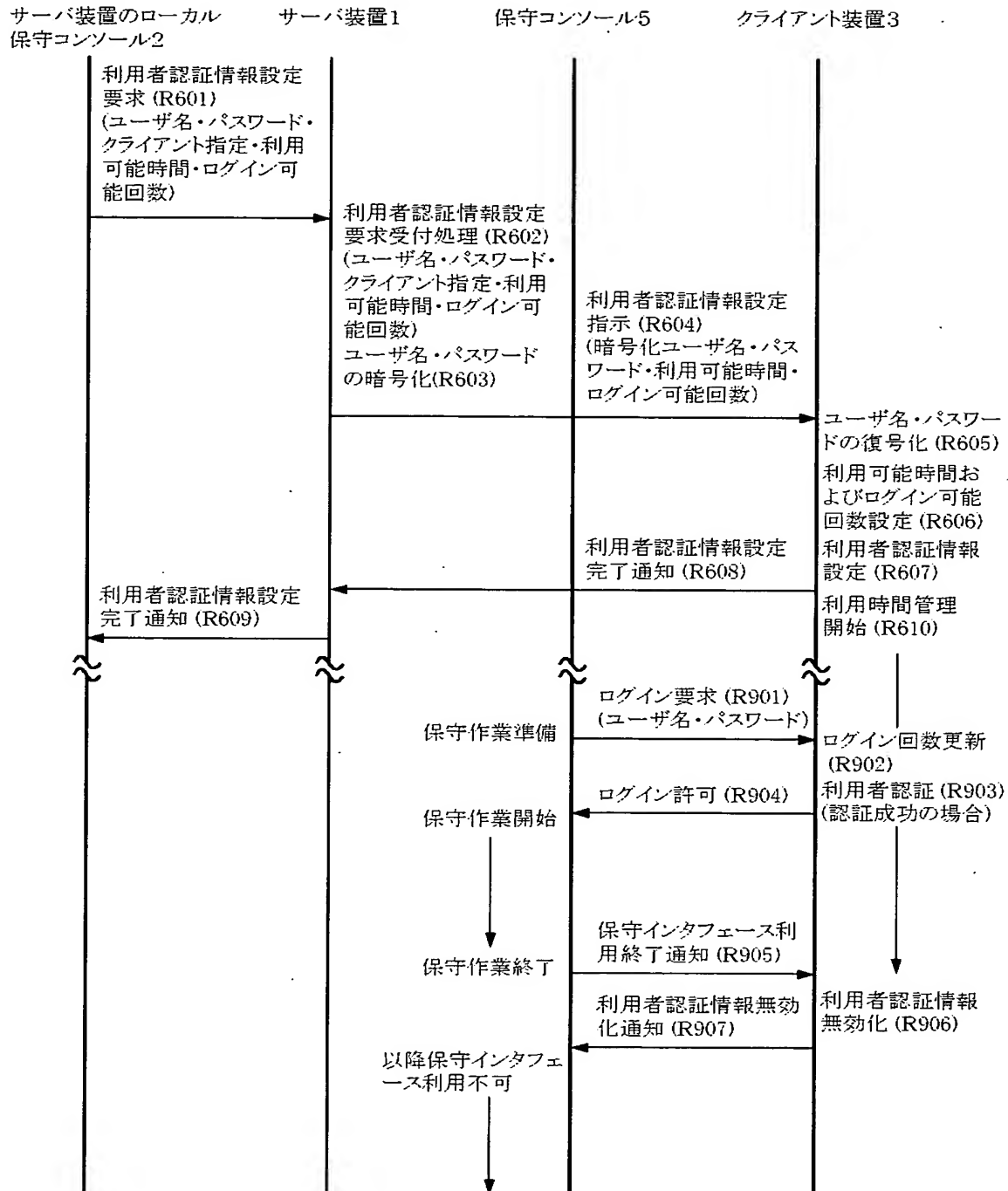
【図 36】

【図 36】



【図 37】

【図 37】



【書類名】 要約書

【要約】

【課題】 クライアント・サーバ型分散システムにおいて、クライアント装置の保守インタフェースの開放、閉塞をサーバ装置から遠隔で行えるようにする。

【解決の手段】 サーバ装置 1 の要求受付部 1 1 は、サーバ側コンソール 2 から、利用者認証情報とクライアント装置 3 の指定とを含む報設定要求、クライアント装置 3 の指定を含む設定無効要求を受け付け、要求転送部 1 2 は L A N 6 を通じて指定されたクライアント装置 3 に転送する。クライアント装置 3 のリモート要求処理部 3 3 は、受信した設定要求中の利用者認証情報を、保守インタフェース 3 0 を利用する利用者の認証を行う利用者認証部 3 2 に設定し、保守インタフェース 3 0 を開放する。また、設定無効要求を受信したときは、利用者認証部 3 2 に設定されている利用者認証情報を無効にして保守インタフェース 3 0 を閉塞する。

【選択図】 図 1

特願 2 0 0 2 - 3 5 6 8 3 9

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1. 変更年月日
[変更理由]

1 9 9 0 年 8 月 2 9 日
新規登録

住 所
氏 名

東京都港区芝五丁目 7 番 1 号
日本電気株式会社